COMISIÓN
EUROPEA

Bruselas, 24.9.2020
COM(2020) 595 final

2020/0266 (COD)

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014 y (UE) n.º 909/2014

(Texto pertinente a efectos del EEE)

{SEC(2020) 307 final} - {SWD(2020) 198 final} - {SWD(2020) 199 final}

EXPOSICIÓN DE MOTIVOS

1. CONTEXTO DE LA PROPUESTA

- Razones y objetivos de la propuesta

La presente propuesta forma parte del paquete de finanzas digitales, un paquete de medidas para seguir propiciando y apoyando el potencial de las finanzas digitales en términos de innovación y competencia, mitigando al mismo tiempo los riesgos que se derivan de ella. Está en consonancia con las prioridades de la Comisión de hacer que Europa esté adaptada a la era digital y construir una economía preparada para el futuro y al servicio de las personas. El paquete de finanzas digitales incluye una nueva Estrategia sobre finanzas digitales para el sector financiero de la UE[1] con el objetivo de garantizar que la Unión adopte la revolución digital y la impulse con empresas europeas innovadoras en la vanguardia, poniendo los beneficios de las finanzas digitales a disposición de los consumidores y las empresas. Además de esta propuesta, el paquete incluye también una propuesta de Reglamento relativo a los mercados de criptoactivos[2], una propuesta de Reglamento sobre un régimen piloto de las infraestructuras del mercado basadas en la tecnología de registro descentralizado (TRD) [3] y una propuesta de Directiva para aclarar o modificar determinadas normas conexas de la UE en materia de servicios financieros[4]. La digitalización y la resiliencia operativa en el sector financiero son dos caras de la misma moneda. Las tecnologías digitales o de la información y la comunicación (TIC) presentan tanto oportunidades como riesgos, que deben ser bien comprendidos y gestionados, especialmente en momentos de tensión.

Por lo tanto, los responsables políticos y los supervisores se han centrado cada vez más en los riesgos derivados de la dependencia de las TIC. En particular, han intentado aumentar la resiliencia de las empresas mediante el establecimiento de normas y la coordinación del trabajo de regulación o supervisión. Este trabajo se ha llevado a cabo tanto a escala internacional como europea, y tanto a nivel intersectorial como en una serie de sectores específicos, incluidos los servicios financieros.

No obstante, los riesgos de TIC siguen planteando un reto para la resiliencia operativa, el funcionamiento y la estabilidad del sistema financiero de la UE. La reforma que siguió a la crisis financiera de 2008 reforzó principalmente la resiliencia financiera[5] del sector financiero de la UE, abordando únicamente los riesgos de TIC de forma indirecta en algunos ámbitos, como parte de las medidas para abordar los riesgos operativos de manera más general.

Aunque los cambios posteriores a la crisis en la legislación de la UE en materia de servicios financieros establecieron un código normativo único que contempla gran parte de los riesgos financieros asociados a los servicios financieros, no abordaron plenamente la resiliencia

---

1 Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Banco Central Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre una Estrategia de Finanzas Digitales para la UE, 23 de septiembre de 2020, COM(2020) 591.

2 Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los mercados de criptoactivos y por el que se modifica la Directiva (UE) 2019/1937, COM(2020) 593

3 Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a un régimen piloto de las infraestructuras del mercado basadas en la tecnología de registro descentralizado, COM (2020) 594.

4 Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se modifican las Directivas 2006/43/CE, 2009/65/CE, 2009/138/UE, 2011/61/UE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366 y (UE) 2016/2341, COM (2020) 596.

5 Las diferentes medidas adoptadas tenían fundamentalmente por objeto aumentar los recursos de capital y la liquidez de las entidades financieras, así como reducir los riesgos de mercado y de crédito.

operativa digital. Las medidas adoptadas en relación con esta última tenían una serie de características que limitaban su eficacia. Por ejemplo, a menudo se concibieron como directivas de armonización mínima o reglamentos basados en principios, lo que dejaba un margen considerable para enfoques divergentes en todo el mercado único. Además, solo se ha prestado una atención limitada o incompleta a los riesgos de TIC en el contexto de la cobertura del riesgo operativo. Por último, estas medidas varían en función de la legislación sectorial sobre servicios financieros. Así pues, la intervención a escala de la Unión no se ajustó plenamente a lo que las entidades financieras europeas necesitan para gestionar los riesgos operativos de tal manera que resistan los incidentes relacionados con las TIC, respondan a ellos y se recuperen de su impacto. Tampoco proporcionó a los supervisores financieros las herramientas más adecuadas para cumplir sus mandatos de evitar la inestabilidad financiera derivada de la materialización de esos riesgos de TIC.

La ausencia de normas detalladas y exhaustivas sobre la resiliencia operativa digital a escala de la UE ha dado lugar a la proliferación de iniciativas reguladoras nacionales (por ejemplo, sobre pruebas de resiliencia operativa digital) y enfoques de supervisión (que se centran, por ejemplo, en las dependencias de terceros en relación a las TIC). Sin embargo, la acción a nivel de los Estados miembros solo tiene un efecto limitado dada la naturaleza transfronteriza de los riesgos de TIC. Por otra parte, las iniciativas nacionales descoordinadas han dado lugar a solapamientos, incoherencias, requisitos duplicados, elevados costes administrativos y de cumplimiento —especialmente para las entidades financieras transfronterizas— o riesgos de TIC aún no detectados y, por tanto, no subsanados. Esta situación fragmenta el mercado único, socava la estabilidad e integridad del sector financiero de la UE y pone en peligro la protección de los consumidores y los inversores.

Por consiguiente, es necesario establecer un marco detallado y exhaustivo sobre la resiliencia operativa digital de las entidades financieras de la UE. Este marco profundizará la dimensión de gestión del riesgo digital del código normativo único. En particular, mejorará y racionalizará la gestión de los riesgos de TIC por parte de las entidades financieras, establecerá pruebas exhaustivas de los sistemas de TIC, aumentará la concienciación de los supervisores sobre los riesgos cibernéticos y los incidentes relacionados con las TIC a los que se enfrentan las entidades financieras, y facultará a los supervisores financieros para supervisar los riesgos derivados de la dependencia de proveedores terceros de servicios de TIC por parte de las entidades financieras. La propuesta creará un mecanismo coherente de notificación de incidentes que contribuirá a reducir las cargas administrativas para las entidades financieras y reforzará la eficacia de la supervisión.

- Coherencia con las disposiciones existentes en la misma política sectorial

La presente propuesta forma parte de una labor más amplia en curso a escala europea e internacional para reforzar la ciberseguridad de los servicios financieros y abordar riesgos operativos más amplios[6].

También responde al dictamen técnico conjunto[7] de las Autoridades Europeas de Supervisión (AES) de 2019, que abogaba por un enfoque más coherente a la hora de abordar el riesgo de

[6] Comité de Supervisión Bancaria de Basilea, *Cyber-resilience: Range of practices* [«Ciberresiliencia: conjunto de prácticas», documento en inglés], diciembre de 2018 y *Principles for sound management of operational risk (PSMOR)* [«Principios para una buena gestión del riesgo operativo», documento en inglés], octubre de 2014.

[7] Dictamen conjunto de las Autoridades Europeas de Supervisión a la Comisión Europea sobre la necesidad de introducir mejoras legislativas en relación con los requisitos de gestión de los riesgos de TIC en el sector financiero de la UE, JC 2019 26.

TIC en las finanzas y recomendaba a la Comisión que reforzara, de manera proporcionada, la resiliencia operativa digital del sector de los servicios financieros a través de una iniciativa sectorial de la UE. El dictamen de las AES era una respuesta al Plan de Acción en materia de Tecnología Financiera de la Comisión de 2018 [8].

- Coherencia con otras políticas de la Unión

Tal como declaró la presidenta Von der Leyen en sus Orientaciones políticas[9], y como se expone en la Comunicación «Configurar el futuro digital de Europa»[10], es fundamental que Europa aproveche todos los beneficios de la era digital y refuerce su industria y su capacidad de innovación, dentro de unos límites seguros y éticos. La Estrategia Europea de Datos[11] establece cuatro pilares (protección de datos, derechos fundamentales, seguridad y ciberseguridad) como requisitos previos esenciales para una sociedad empoderada por el uso de datos. Más recientemente, el Parlamento Europeo ha venido trabajando en un informe sobre las finanzas digitales, que, entre otras cosas, pide un enfoque común sobre la ciberresiliencia del sector financiero[12]. Un marco legislativo que refuerce la resiliencia operativa digital de las entidades financieras de la UE es coherente con estos objetivos. La propuesta también apoyaría las políticas de recuperación tras el coronavirus, ya que garantizaría que la mayor dependencia de las finanzas digitales vaya acompañada de la resiliencia operativa.

La iniciativa preservaría los beneficios asociados al marco horizontal en materia de ciberseguridad (por ejemplo, la Directiva relativa a la seguridad de las redes y sistemas de información, Directiva SRI), al mantener al sector financiero dentro de su ámbito de aplicación. El sector financiero seguiría estando estrechamente asociado al organismo de cooperación SRI y los supervisores financieros podrían intercambiar información pertinente dentro del actual ecosistema SRI. La iniciativa sería coherente con la Directiva sobre infraestructuras críticas europeas (ICE), que se está revisando actualmente para mejorar la protección y la resiliencia de las infraestructuras críticas frente a las amenazas no cibernéticas. Por último, la presente propuesta está plenamente en consonancia con la Estrategia para una Unión de la Seguridad[13], que abogaba por una iniciativa sobre la resiliencia operativa digital del sector financiero, dada su gran dependencia de los servicios de TIC y su elevada vulnerabilidad a los ciberataques.

---

8 Comisión Europea, Plan de Acción en materia de Tecnología Financiera, COM(2018) 0109 final.

9 Presidenta Ursula von der Leyen, Orientaciones políticas para la próxima Comisión Europea 2019-2024, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf.

10 Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, «Configurar el futuro digital de Europa», COM(2020) 67 final.

11 Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, «Una estrategia europea de datos», COM(2020) 66 final.

12 «Report with recommendations to the Commission on Digital Finance:
emerging risks in crypto-assets - regulatory and supervisory challenges in the area of financial services, institutions and markets» [«Informe con recomendaciones destinadas a la Comisión sobre las finanzas digitales: riesgos emergentes en criptoactivos: retos reglamentarios y de supervisión en el ámbito de los servicios, las instituciones y los mercados financieros», documento en inglés], [2020/2034 (INL)],, https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2034(INL)&l=en

13 Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la Estrategia de la UE para una Unión de la Seguridad, COM(2020) 605 final.

2. BASE JURÍDICA, SUBSIDIARIEDAD Y PROPORCIONALIDAD

- Base jurídica

La presente propuesta de Reglamento se basa en el artículo 114 del TFUE.

Elimina obstáculos al mercado interior de servicios financieros y mejora su establecimiento y funcionamiento armonizando las normas aplicables en el ámbito de la gestión del riesgo de TIC, la presentación de informes, las pruebas y el riesgo de terceros relacionado con las TIC. Las disparidades actuales en este ámbito, tanto a nivel legislativo como de supervisión, así como a nivel nacional y de la UE, obstaculizan el mercado único de servicios financieros, ya que las entidades financieras que realizan actividades transfronterizas se enfrentan a requisitos reguladores o expectativas de supervisión diferentes o que se solapan, y que pueden obstaculizar el ejercicio de sus libertades de establecimiento y de prestación de servicios. La existencia de normas diferentes también falsea la competencia entre el mismo tipo de entidades financieras en diferentes Estados miembros. Además, en ámbitos en los que no hay armonización, o esta es parcial o limitada, el desarrollo de normas o enfoques nacionales divergentes, ya en vigor o en proceso de adopción y aplicación a nivel nacional, puede tener un efecto disuasorio para las libertades del mercado único de servicios financieros. Este es el caso, en particular, de los marcos de pruebas operativas digitales y la supervisión de proveedores terceros esenciales de servicios de TIC.

Dado que la propuesta incide en varias Directivas del Parlamento Europeo y del Consejo adoptadas sobre la base del artículo 53, apartado 1, del TFUE, al mismo tiempo se adopta una propuesta de Directiva para reflejar las modificaciones necesarias de dichas Directivas.

- Subsidiariedad

Un alto grado de interconexión entre los servicios financieros, una importante actividad transfronteriza de las entidades financieras y una amplia dependencia del sector financiero en su conjunto de proveedores terceros de servicios de TIC requieren que se propicie una sólida resiliencia operativa digital como cuestión de interés común para mantener la solidez de los mercados financieros de la UE. Las disparidades resultantes de regímenes desiguales o parciales, solapamientos o requisitos múltiples aplicables a las mismas entidades financieras que operan a escala transfronteriza o que poseen varias autorizaciones[14] en el mercado único solo pueden abordarse eficazmente a escala de la Unión.

La presente propuesta armoniza el componente operativo digital de un sector profundamente integrado e interconectado que ya se beneficia de un conjunto único de normas y está sujeto a supervisión en la mayoría de los demás ámbitos clave. En cuestiones como la notificación de incidentes relacionados con las TIC, solo las normas armonizadas de la Unión podrían reducir el nivel de cargas administrativas y los costes financieros asociados a la notificación de un mismo incidente relacionado con las TIC a diferentes autoridades nacionales y de la Unión. La acción de la UE también es necesaria para facilitar el reconocimiento mutuo de los resultados de las pruebas avanzadas de resiliencia operativa digital para las entidades que operan a escala transfronteriza, que, en ausencia de normas de la Unión, están o pueden estar sujetas a marcos diferentes en los distintos Estados miembros. Solo una acción a nivel de la Unión puede solventar las diferencias en los enfoques de pruebas introducidas por los Estados

[14] La misma entidad financiera puede tener sendas licencias de entidad bancaria, empresa de servicios de inversión y entidad de pago, cada una de ellas expedida por un supervisor diferente en uno o varios Estados miembros.

miembros. También es necesaria una actuación a escala de la UE para abordar la falta de facultades de supervisión adecuadas para controlar los riesgos derivados de los proveedores terceros de servicios de TIC, incluidos los riesgos de concentración y de contagio para el sector financiero de la UE.

- Proporcionalidad

Las normas propuestas no van más allá de lo necesario para alcanzar los objetivos de la propuesta. Solo cubren los aspectos que los Estados miembros no pueden alcanzar por sí solos y en los que la carga administrativa y los costes son proporcionados a los objetivos específicos y generales que deben alcanzarse.

La proporcionalidad está concebida en términos de alcance e intensidad mediante el uso de criterios de evaluación cualitativos y cuantitativos. Su objetivo es garantizar que, aunque las nuevas normas cubran a todas las entidades financieras, estén al mismo tiempo adaptadas a los riesgos y necesidades de sus características específicas en términos de tamaño y perfiles empresariales. La proporcionalidad también está integrada en las normas sobre gestión del riesgo de TIC, las pruebas de resiliencia digital, la notificación de incidentes graves relacionados con las TIC y la supervisión de proveedores terceros esenciales de servicios de TIC.

- Elección del instrumento

Las medidas necesarias para regular la gestión del riesgo de TIC, la notificación de incidentes relacionados con las TIC, las pruebas y la supervisión de los proveedores terceros esenciales de servicios de TIC deben incluirse en un reglamento a fin de garantizar que los requisitos detallados sean efectiva y directamente aplicables de manera uniforme, sin perjuicio de la proporcionalidad y las normas específicas previstas en el presente Reglamento. La coherencia a la hora de abordar los riesgos operativos digitales contribuye a aumentar la confianza en el sistema financiero y preserva su estabilidad. Dado que el uso de un reglamento ayuda a reducir la complejidad normativa, fomenta la convergencia en materia de supervisión y aumenta la seguridad jurídica, el presente Reglamento también contribuye a limitar los costes de cumplimiento de las entidades financieras, especialmente de las que operan a escala transfronteriza, lo que, a su vez, contribuiría a eliminar los falseamientos de la competencia.

El presente Reglamento también elimina las disparidades legislativas y los enfoques reguladores o de supervisión nacionales desiguales del riesgo de TIC, eliminando así los obstáculos al mercado único de los servicios financieros, en particular para el correcto ejercicio de la libertad de establecimiento y prestación de servicios por las entidades financieras con presencia transfronteriza.

Por último, el código normativo único se ha desarrollado principalmente a través de reglamentos, por lo que debe elegirse el mismo instrumento jurídico con vistas a su actualización con el componente de resiliencia operativa digital.

3. RESULTADOS DE LAS EVALUACIONES EX POST, DE LAS CONSULTAS CON LAS PARTES INTERESADAS Y DE LAS EVALUACIONES DE IMPACTO

- Evaluaciones *ex post* / controles de calidad de la legislación existente

Hasta ahora, ningún texto legislativo de la Unión en materia de servicios financieros se ha centrado en la resiliencia operativa y ninguno ha abordado de forma exhaustiva los riesgos

derivados de la digitalización, ni siquiera aquellos cuyas normas abordan de manera más general la dimensión del riesgo operativo con el riesgo de TIC como subcomponente. La intervención de la Unión ha contribuido hasta ahora a abordar las necesidades y los problemas que surgieron tras la crisis financiera de 2008: las entidades de crédito no estaban suficientemente capitalizadas, los mercados financieros no estaban suficientemente integrados y la armonización hasta ese momento se había mantenido en mínimos. Entonces no se consideró prioritario el riesgo de TIC y, como consecuencia de ello, los marcos jurídicos de los distintos subsectores financieros han evolucionado de manera descoordinada. Sin embargo, la acción de la Unión ha logrado sus objetivos de garantizar la estabilidad financiera y de establecer un conjunto único de normas prudenciales y de conducta de mercado armonizadas y aplicables a las entidades financieras en toda la UE. Dado que los factores que impulsaron la intervención legislativa de la Unión en el pasado no permitieron regular, mediante normas específicas o exhaustivas, el uso generalizado de las tecnologías digitales y los consiguientes riesgos en las finanzas, la realización de una evaluación explícita parece difícil. En cada pilar del presente Reglamento se reflejan un ejercicio de evaluación implícito y las consiguientes modificaciones legislativas.

- Consultas con las partes interesadas

La Comisión ha consultado a las partes interesadas a lo largo de todo el proceso de elaboración de la presente propuesta, en particular:

i) La Comisión llevó a cabo una consulta pública abierta específica (del 19 de diciembre de 2019 al 19 de marzo de 2020) [15];

ii) La Comisión consultó al público mediante una evaluación de impacto inicial (del 19 de diciembre de 2019 al 16 de enero de 2020) [16];

iii) Los servicios de la Comisión consultaron a expertos de los Estados miembros en el Grupo de Expertos en Banca, Pagos y Seguros en dos ocasiones (18 de mayo de 2020 y 16 de julio de 2020) [17];

iv) Los servicios de la Comisión celebraron, el 19 de mayo de 2020, un seminario web específico sobre la resiliencia operativa digital, como parte de la serie de actos de divulgación de las finanzas digitales de 2020.

El objetivo de la consulta pública era informar a la Comisión sobre el desarrollo de un posible marco de resiliencia operativa digital intersectorial de la UE en el ámbito de los servicios financieros. Las respuestas mostraron un amplio apoyo a la introducción de un marco específico con acciones centradas en los cuatro ámbitos objeto de la consulta, subrayando al mismo tiempo la necesidad de garantizar la proporcionalidad y de tener en cuenta y explicar cuidadosamente la interacción con las normas horizontales de la Directiva SRI. La Comisión recibió dos respuestas sobre la evaluación de impacto inicial, en las que los encuestados abordaban aspectos específicos relacionados con su ámbito de actividad.

[15] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-/public-consultation

[16] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-

[17] https://ec.europa.eu/info/business-economy-euro/banking-and-finance/regulatory-process-financial-services/expert-groups-comitology-and-other-committees/expert-group-banking-payments-and-insurance_en

Los Estados miembros expresaron en la reunión del Grupo de Expertos en Banca, Pagos y Seguros celebrada el 18 de mayo de 2020 un gran apoyo al refuerzo de la resiliencia operativa digital del sector financiero a través de las acciones previstas en torno a los cuatro elementos señalados por la Comisión. Los Estados miembros también destacaron la necesidad de articular claramente las nuevas normas con las relativas al riesgo operativo (dentro de la legislación de la UE en materia de servicios financieros) y con las normas horizontales sobre ciberseguridad (Directiva SRI). Durante la segunda reunión, algunos Estados miembros destacaron la necesidad de garantizar la proporcionalidad y de considerar la situación específica de las pequeñas empresas o de las filiales de grupos más grandes, así como la necesidad de contar con un mandato sólido para las autoridades nacionales competentes que participan en la supervisión.

La propuesta también se basa en la información obtenida en las reuniones celebradas con las partes interesadas y las autoridades e instituciones de la UE e integra esta información. Las partes interesadas, incluidos los proveedores terceros de servicios de TIC, en general han mostrado su apoyo. Un análisis de los comentarios recibidos muestra que los interesados abogan por preservar la proporcionalidad y seguir un enfoque basado en principios y riesgos en el diseño de las normas. Desde el punto de vista institucional, las principales aportaciones procedieron de la Junta Europea de Riesgo Sistémico (JERS), las AES, la Agencia de la Unión Europea para la Ciberseguridad (ENISA) y el Banco Central Europeo (BCE), así como de las autoridades competentes de los Estados miembros.

- Obtención y uso de asesoramiento especializado

Al preparar la presente propuesta, la Comisión se basó en datos cualitativos y cuantitativos obtenidos de fuentes reconocidas, incluidos los dos dictámenes técnicos conjuntos de las AES. Esto se ha complementado con aportaciones confidenciales e informes a disposición del público de las autoridades de supervisión, los organismos internacionales de normalización y los principales institutos de investigación, así como con aportaciones cuantitativas y cualitativas de partes interesadas de todo el sector financiero mundial.

- Evaluación de impacto

La presente propuesta va acompañada de una evaluación de impacto[18], que se presentó al Comité de Control Reglamentario el 29 de abril de 2020 y se aprobó el 29 de mayo de 2020. El Comité de Control Reglamentario recomendó mejoras en algunos ámbitos con vistas a: i) proporcionar más información sobre cómo se garantizaría la proporcionalidad; ii) destacar mejor en qué medida la opción preferida difiere del asesoramiento técnico conjunto de las AES y por qué esa opción es la óptima; y iii) destacar más cómo interactúa la propuesta con la legislación vigente de la UE, incluidas las normas que se están revisando actualmente. La evaluación de impacto se ajustó para abordar estos puntos, atendiendo también a las observaciones más detalladas del Comité de Control Reglamentario.

La Comisión estudió una serie de opciones de actuación para desarrollar un marco de resiliencia operativa digital:

[18] Documento de trabajo de los servicios de la Comisión —Informe de evaluación de impacto que acompaña al documento Reglamento del Parlamento Europeo y del Consejo sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014 y (UE) n.º 909/2014, SWD (2020) 198 de 24.9.2020.

- «No hacer nada»: las normas sobre resiliencia operativa seguirían estando establecidas por el actual conjunto divergente de disposiciones en materia de servicios financieros de la UE, en parte por la Directiva SRI, y por los regímenes nacionales actuales o futuros.
- Opción 1: reforzar los colchones de capital: se introducirían colchones de capital adicionales para aumentar la capacidad de las entidades financieras de absorber las pérdidas que podrían derivarse de la falta de resiliencia operativa digital.
- Opción 2: adoptar un texto legislativo sobre resiliencia operativa digital en el ámbito de los servicios financieros, que prevea un marco exhaustivo a escala de la UE con normas coherentes que aborden las necesidades de resiliencia operativa digital de todas las entidades financieras reguladas y establezca un marco de supervisión para proveedores terceros esenciales de servicios de TIC.
- Opción 3: un texto legislativo sobre resiliencia operativa digital en el ámbito de los servicios financieros combinado con una supervisión centralizada de los proveedores terceros esenciales de servicios de TIC: además de un texto legislativo sobre resiliencia operativa digital (opción 2), se establecería una nueva autoridad para supervisar la prestación de servicios por proveedores terceros de servicios de TIC.

Se eligió la segunda opción, ya que logra la mayoría de los objetivos previstos de manera eficaz, eficiente y coherente con otras políticas de la Unión. La mayoría de las partes interesadas también prefieren esta opción.

La opción elegida generaría costes tanto puntuales como recurrentes[19]. Los costes puntuales se deben principalmente a las inversiones en sistemas informáticos y, como tales, son difíciles de cuantificar, dado el diferente estado de los complejos entornos informáticos de las empresas y, en particular, de sus sistemas informáticos heredados. Aun así, es probable que estos costes sean limitados para las grandes empresas, habida cuenta de las importantes inversiones en TIC que ya han realizado. También se espera que los costes sean limitados para las empresas más pequeñas, ya que se aplicarían medidas proporcionadas debido a su menor riesgo.

La opción elegida tendría efectos positivos para las pymes que operan en el sector de los servicios financieros en términos de impacto económico, social y medioambiental. La propuesta aportará claridad a las pymes sobre qué normas se aplican, lo que reducirá los costes de cumplimiento.

La opción elegida repercutiría a nivel social principalmente en los consumidores y los inversores. Unos niveles más elevados de resiliencia operativa digital del sistema financiero de la UE reducirían el número y los costes medios de los incidentes. La sociedad en su conjunto se beneficiaría del aumento de la confianza en el sector de los servicios financieros.

Por último, en términos de impacto medioambiental, la opción elegida fomentaría un mayor uso de la última generación de infraestructuras y servicios de TIC, que se espera sean más sostenibles desde el punto de vista medioambiental.

- Adecuación regulatoria y simplificación

[19] *Ibidem*, p. 89.

La supresión del solapamiento de los requisitos de notificación de incidentes relacionados con las TIC reduciría las cargas administrativas y los costes asociados. Además, las pruebas de resiliencia operativa digital armonizadas, con reconocimiento mutuo en todo el mercado único, reducirán los costes, especialmente para las empresas transfronterizas que, de otro modo, podrían tener que realizar múltiples pruebas en distintos Estados miembros[20].

- Derechos fundamentales

La UE se ha comprometido a garantizar un alto nivel de protección de los derechos fundamentales. Todos los acuerdos voluntarios de intercambio de información entre entidades financieras que promueve el presente Reglamento se llevarían a cabo en entornos de confianza respetando plenamente las normas de protección de datos de la Unión, en particular el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo[21], en particular cuando el tratamiento de datos personales sea necesario para satisfacer un interés legítimo perseguido por el responsable del tratamiento de los datos.

4. REPERCUSIONES PRESUPUESTARIAS

En cuanto a las implicaciones presupuestarias, dado que el Reglamento actual prevé un papel reforzado de las AES mediante las facultades que les son conferidas para supervisar adecuadamente a proveedores terceros esenciales de TIC, la propuesta implicaría el despliegue de más recursos, en particular para cumplir las misiones de supervisión (como las inspecciones *in situ* y en línea y los ejercicios de auditoría), y el uso de personal que posea conocimientos técnicos en materia de seguridad de las TIC.

La magnitud y distribución de estos costes dependerá del alcance de las nuevas facultades de supervisión y de las tareas (precisas) que deban desempeñar las AES. En términos de dotación de nuevos recursos de personal, la ABE, la AEVM y la AESPJ necesitarán un total de 18 puestos equivalentes a jornada completa (EJC) —6 EJC por cada autoridad— cuando entren en vigor las diferentes disposiciones de la propuesta (con un coste estimado en 15,71 millones EUR para el período 2022-2027). Las AES también incurrirán en costes informáticos adicionales, gastos de misión para las inspecciones *in situ* y costes de traducción (estimados en 12 millones EUR para el período 2022-2027), así como otros gastos administrativos (estimados en 2,48 millones EUR para el período 2022-2027). Por lo tanto, el impacto del coste total estimado es de aproximadamente 30,19 millones EUR para el período 2022-2027.

Cabe señalar también que, si bien los efectivos (por ejemplo, nuevos miembros del personal y otros gastos relacionados con las nuevas tareas) necesarios para la supervisión directa dependerán a lo largo del tiempo de la evolución del número y el tamaño de los proveedores terceros esenciales de servicios de TIC que deban supervisarse, los gastos respectivos se financiarán íntegramente con las tasas cobradas a dichos participantes en el mercado. Por lo tanto, no se prevé ningún impacto en los créditos presupuestarios de la UE (excepto en cuanto al personal adicional), ya que estos costes se financiarán íntegramente mediante tasas.

La incidencia presupuestaria y financiera de la presente propuesta se explica en detalle en la ficha financiera legislativa adjunta.

---

20 *Ibidem*..

21 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) (DO L 119 de 4.5.2016, p. 1).

5. OTROS ELEMENTOS

- Planes de ejecución y modalidades de seguimiento, evaluación e información

La propuesta incluye un plan general de seguimiento y evaluación del impacto en los objetivos específicos, que requiere que la Comisión lleve a cabo una revisión al menos tres años después de la entrada en vigor e informe al Parlamento Europeo y al Consejo de sus principales conclusiones.

La revisión debe llevarse a cabo de forma acorde con las Directrices de la Comisión para la mejora de la legislación.

- Explicación detallada de las disposiciones específicas de la propuesta

La propuesta está estructurada en torno a varios ámbitos de actuación principales que son pilares clave interrelacionados incluidos de forma consensuada en las orientaciones y buenas prácticas europeas e internacionales destinadas a mejorar la resiliencia cibernética y operativa del sector financiero.

Ámbito de aplicación del Reglamento y proporcionalidad en la aplicación de las medidas exigidas (artículo 2)

Para garantizar la coherencia de los requisitos de gestión del riesgo de TIC aplicables al sector financiero, el Reglamento abarca una serie de entidades financieras reguladas a escala de la Unión, a saber, entidades de crédito, entidades de pago, entidades de dinero electrónico, empresas de servicios de inversión, proveedores de servicios de criptoactivos, depositarios centrales de valores, entidades de contrapartida central, centros de negociación, registros de operaciones, gestores de fondos de inversión alternativos y sociedades de gestión, proveedores de servicios de suministro de datos, empresas de seguros y reaseguros, intermediarios de seguros, intermediarios de reaseguros e intermediarios de seguros complementarios, fondos de pensiones de empleo, agencias de calificación crediticia, auditores legales y sociedades de auditoría, administradores de índices de referencia cruciales y proveedores de servicios de financiación participativa.

Esta cobertura facilita una aplicación homogénea y coherente de todos los componentes de la gestión de riesgos en ámbitos relacionados con las TIC, salvaguardando al mismo tiempo la igualdad de condiciones entre las entidades financieras con respecto a sus obligaciones reglamentarias en materia de riesgo de TIC. Al mismo tiempo, el Reglamento reconoce que existen diferencias significativas entre las entidades financieras en términos de tamaño, perfiles empresariales o en relación con su exposición al riesgo digital. Dado que las entidades financieras de mayor tamaño disponen de más recursos, solo las entidades financieras que no reúnan las condiciones para ser consideradas microempresas están obligadas, por ejemplo, a establecer sistemas de gobernanza complejos o funciones de gestión específicas, realizar evaluaciones en profundidad tras cambios importantes en las infraestructuras de redes y sistemas de información, realizar periódicamente análisis de riesgos sobre los sistemas de TIC heredados, y ampliar las pruebas a las que se someten los planes de continuidad de la actividad y de respuesta y recuperación para reflejar los escenarios de conmutación entre su infraestructura primaria de TIC y sus instalaciones redundantes. Además, solo se exigirá a las entidades financieras consideradas significativas a efectos de las pruebas avanzadas de resiliencia digital que lleven a cabo pruebas de penetración guiadas por amenazas («TLPT», por sus siglas en inglés).

A pesar de que la cobertura es amplia, no es exhaustiva. En particular, el presente Reglamento no incluye a los operadores de los sistemas, tal como se definen en el artículo 2, letra p), de la Directiva 98/26/CE[22] sobre la firmeza de la liquidación en los sistemas de pagos y de liquidación de valores, ni a ningún participante en el sistema, a menos que dicho participante sea una entidad financiera regulada a nivel de la Unión y, como tal, esté cubierta por el presente Reglamento por derecho propio (es decir, entidad de crédito, empresa de servicios de inversión, entidad de contrapartida central). Además, el registro de derechos de emisión de la Unión que funciona, de conformidad con la Directiva 2003/87/CE[23], bajo los auspicios de la Comisión Europea también está fuera del ámbito de aplicación.

Estas exclusiones de la Directiva sobre la firmeza de la liquidación tienen en cuenta la necesidad de examinar más detenidamente las cuestiones jurídicas y estratégicas que afectan a los participantes y a los operadores de sistemas contemplados en dicha Directiva, al tiempo que se tiene debidamente en cuenta el impacto de los marcos que se aplican actualmente a los sistemas de pago[24] gestionados por los bancos centrales. Dado que estas cuestiones pueden implicar aspectos que siguen siendo distintos de los cubiertos por el presente Reglamento, la Comisión seguirá evaluando la necesidad y el impacto de una nueva ampliación del ámbito de aplicación del presente Reglamento a entidades e infraestructuras de TIC que actualmente están fuera de él.

Requisitos relacionados con la gobernanza (artículo 4)

El presente Reglamento tiene por objeto armonizar más las estrategias empresariales de las entidades financieras y la gestión del riesgo de TIC. A tal efecto, el órgano de dirección estará obligado a mantener un papel crucial y activo en la dirección del marco de gestión de riesgos de TIC y procurará respetar una ciberhigiene estricta. La plena responsabilidad del órgano de dirección en la gestión del riesgo de TIC de la entidad financiera será un principio general que se traducirá en un conjunto de requisitos específicos, como la asignación de cometidos y responsabilidades claros para todas las funciones relacionadas con las TIC, una implicación continua en el control del seguimiento de la gestión del riesgo de TIC, así como en toda la gama de procesos de aprobación y control y una asignación adecuada de inversiones y formación en TIC.

Requisitos de gestión del riesgo de TIC (artículos 5 a 14)

La resiliencia operativa digital se basa en un conjunto de principios y requisitos clave sobre el marco de gestión de riesgos de TIC, en consonancia con el asesoramiento técnico conjunto de las AES. Estos requisitos, inspirados en las normas, directrices y recomendaciones internacionales, nacionales y sectoriales, giran en torno a funciones específicas en la gestión de riesgos de TIC (identificación, protección y prevención, detección, respuesta y recuperación, aprendizaje y evolución, y comunicación). Para poder seguir haciendo frente a la naturaleza cambiante de las ciberamenazas, las entidades financieras deben crear y mantener sistemas y herramientas de TIC resilientes que minimicen el impacto del riesgo de

[22] Directiva 98/26/CE del Parlamento Europeo y del Consejo, de 19 de mayo de 1998, sobre la firmeza de la liquidación en los sistemas de pagos y de liquidación de valores (DO L 166 de 11.6.1998, p. 45).

[23] Directiva 2003/87/CE del Parlamento Europeo y del Consejo, de 13 de octubre de 2003, por la que se establece un régimen para el comercio de derechos de emisión de gases de efecto invernadero en la Comunidad y por la que se modifica la Directiva 96/61/CE del Consejo (DO L 275 de 25.10.2003, p. 32).

[24] En particular, el Reglamento (UE) n.° 795/2014 del Banco Central Europeo, de 3 de julio de 2014, sobre los requisitos de vigilancia de los sistemas de pago de importancia sistémica.

TIC, identificar de forma continua todas las fuentes de riesgo de TIC, establecer medidas de protección y prevención, detectar rápidamente actividades anómalas, poner en marcha políticas específicas y exhaustivas de continuidad de la actividad y planes de recuperación en caso de catástrofe como parte integrante de la política de continuidad de la actividad operativa. Estos últimos componentes son necesarios para una rápida recuperación tras incidentes relacionados con las TIC, en particular ciberataques, limitando los daños y dando prioridad a la reanudación segura de las actividades. El Reglamento no impone por sí mismo una normalización específica, sino que se basa en normas técnicas europeas e internacionalmente reconocidas o en las buenas prácticas del sector, en la medida en que se ajustan plenamente a las instrucciones de supervisión sobre el uso y la incorporación de dichas normas internacionales. El presente Reglamento también cubre la integridad, la seguridad y la resiliencia de las infraestructuras e instalaciones físicas que sustentan el uso de la tecnología y los procesos y personas pertinentes relacionados con las TIC, como parte de la huella digital de las operaciones de una entidad financiera.

Notificación de incidentes relacionados con las TIC (artículos 15 a 20)

La armonización y racionalización de la notificación de incidentes relacionados con las TIC se logra mediante, en primer lugar, el requisito general de que las entidades financieras establezcan y apliquen un proceso de gestión para controlar y registrar los incidentes relacionados con las TIC, seguido de la obligación de clasificarlos sobre la base de criterios detallados en el Reglamento y desarrollados en mayor medida por las AES a través de la especificación de umbrales de importancia relativa. En segundo lugar, solo deben notificarse a las autoridades competentes los incidentes relacionados con las TIC que se consideren graves. Los informes deben procesarse utilizando una plantilla común y siguiendo un procedimiento armonizado, ambos desarrollados por las AES. Las entidades financieras deben presentar informes iniciales, intermedios y finales e informar a sus usuarios y clientes cuando el incidente tenga o pueda tener un impacto en sus intereses financieros. Las autoridades competentes deben proporcionar detalles pertinentes de los incidentes a otras instancias o autoridades: a las AES, al BCE y a las ventanillas únicas designadas en virtud de la Directiva (UE) 2016/1148.

Para entablar un diálogo entre las entidades financieras y las autoridades competentes que contribuya a minimizar el impacto y a identificar soluciones adecuadas, la notificación de incidentes graves relacionados con las TIC debe complementarse con información de retorno y orientaciones de los supervisores.

Por último, la posibilidad de centralizar a escala de la Unión la notificación de incidentes relacionados con las TIC debe seguir estudiándose en un informe conjunto de las AES, el BCE y la ENISA en el que se evalúe la viabilidad de crear un único centro de la UE para la notificación de incidentes graves relacionados con las TIC por parte de las entidades financieras.

Pruebas de resiliencia operativa digital (artículos 21 a 24)

Las capacidades y funciones incluidas en el marco de gestión de riesgos de TIC deben someterse a pruebas periódicas para comprobar su estado de preparación y asegurarse de la detección de carencias, deficiencias o lagunas, así como de la rápida aplicación de medidas correctoras. El presente Reglamento permite una aplicación proporcionada de los requisitos de pruebas de resiliencia operativa digital en función del tamaño y el perfil empresarial y de riesgo de las entidades financieras: aunque todas las entidades deben poner a prueba las herramientas y sistemas de TIC, solo aquellas que las autoridades competentes consideren significativas y maduras en términos cibernéticos (sobre la base de los criterios del presente Reglamento desarrollados en mayor medida por las AES) deben llevar a cabo pruebas

avanzadas basadas en TLPT. El presente Reglamento también establece requisitos para los testadores y el reconocimiento de los resultados de las TLPT en toda la Unión para las entidades financieras que operan en varios Estados miembros.

Riesgo de terceros relacionado con las TIC (artículos 25 a 39)

El Reglamento está concebido para garantizar un seguimiento sólido del riesgo de terceros relacionado con las TIC. Este objetivo se alcanzará, en primer lugar, mediante el respeto de normas basadas en principios aplicables al seguimiento por parte de las entidades financieras de los riesgos derivados de proveedores terceros de TIC. En segundo lugar, el presente Reglamento armoniza los elementos clave del servicio y la relación con proveedores terceros de TIC. Estos elementos abarcan aspectos mínimos que se consideran cruciales para permitir un seguimiento completo por parte de la entidad financiera del riesgo de terceros relacionado con las TIC a lo largo de todas las fases de su relación: celebración, ejecución y rescisión del contrato y etapa poscontractual.

En particular, los contratos que rijan esa relación deberán contener una descripción completa de los servicios, la indicación de los lugares en los que deben procesarse los datos, descripciones completas del nivel de servicio acompañadas de objetivos de rendimiento cuantitativos y cualitativos, disposiciones pertinentes sobre accesibilidad, disponibilidad, integridad, seguridad y protección de los datos personales, y garantías de acceso, recuperación y devolución en caso de fallos de los proveedores terceros de servicios de TIC, plazos de preaviso y obligaciones de información de los proveedores terceros de servicios de TIC, derechos de acceso, inspección y auditoría por parte de la entidad financiera o de un tercero designado, derechos de rescisión claros y estrategias de salida específicas. Además, dado que algunos de estos elementos contractuales pueden normalizarse, el Reglamento promueve el uso voluntario de cláusulas contractuales tipo que la Comisión debe desarrollar para el uso del servicio de computación en nube.

Por último, el Reglamento pretende promover la convergencia de los enfoques de supervisión del riesgo de terceros relacionado con las TIC en el sector financiero sometiendo a los proveedores terceros esenciales de servicios de TIC a un marco de supervisión de la Unión. A través de un nuevo marco legislativo armonizado, la AES designada como supervisor principal de cada proveedor tercero esencial de servicios de TIC queda facultada para garantizar que los proveedores de servicios tecnológicos que desempeñen un papel esencial en el funcionamiento del sector financiero sean objeto de un seguimiento adecuado a escala paneuropea. El marco de supervisión previsto en el presente Reglamento se basa en la arquitectura institucional existente en el ámbito de los servicios financieros, en virtud de la cual el Comité Mixto de las AES garantiza la coordinación intersectorial en cuanto a todos los asuntos relativos al riesgo de TIC, de conformidad con sus funciones en materia de ciberseguridad, con el apoyo del subcomité pertinente (Foro de Supervisión), que lleva a cabo los trabajos preparatorios de las decisiones individuales y las recomendaciones colectivas a los proveedores terceros esenciales de servicios de TIC.

Intercambio de información (artículo 40)

Para sensibilizar sobre el riesgo de TIC, minimizar su propagación y apoyar las capacidades defensivas de las entidades financieras y las técnicas de detección de amenazas, el Reglamento permite a las entidades financieras establecer acuerdos para intercambiar información e inteligencia sobre ciberamenazas.

2020/0266 (COD)

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014 y (UE) n.º 909/2014

(Texto pertinente a efectos del EEE)

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea y, en particular, su artículo 114,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de acto legislativo a los parlamentos nacionales,

Visto el dictamen del Banco Central Europeo[25],

Visto el dictamen del Comité Económico y Social Europeo[26],

De conformidad con el procedimiento legislativo ordinario,

Considerando lo siguiente:

(1) En la era digital, las tecnologías de la información y la comunicación (TIC) sustentan sistemas complejos utilizados en actividades cotidianas de la sociedad. Mantienen el funcionamiento de sectores clave de nuestras economías, incluidas las finanzas, y mejoran el funcionamiento del mercado único. El aumento de la digitalización y la interconexión también amplifica los riesgos de las TIC, haciendo que la sociedad en su conjunto —y el sistema financiero en particular— sea más vulnerable a las ciberamenazas o a las perturbaciones de las TIC. Si bien el uso ubicuo de los sistemas de TIC y la alta digitalización y conectividad son hoy en día características fundamentales de todas las actividades de las entidades financieras de la Unión, la resiliencia digital aún no está suficientemente integrada en sus marcos operativos.

(2) El uso de las TIC ha adquirido en las últimas décadas un papel fundamental en las finanzas, asumiendo hoy una importancia crítica en el desarrollo de las funciones cotidianas típicas de todas las entidades financieras. La digitalización abarca, por ejemplo, los pagos, que han pasado cada vez más de la utilización de efectivo y métodos basados en papel al uso de soluciones digitales, así como la compensación y liquidación de valores, la negociación electrónica y algorítmica, las operaciones de préstamo y financiación, la financiación entre particulares, la calificación crediticia, la suscripción de seguros, la gestión de siniestros y las operaciones administrativas. No solo se ha digitalizado en gran medida todo el sector financiero, sino que la digitalización también ha profundizado las interconexiones y dependencias, tanto dentro de este, como con proveedores terceros de infraestructuras y servicios.

[25] [*Añádase la referencia*] DO C, p..

[26] [*Añádase la referencia*] DO C, p..

(3) La Junta Europea de Riesgo Sistémico (JERS) ha reafirmado en un informe de 2020 sobre el ciberriesgo sistémico[27] que el elevado nivel actual de interconexión entre entidades financieras, mercados financieros e infraestructuras de los mercados financieros, y en particular las interdependencias de sus sistemas de TIC, puede constituir una vulnerabilidad sistémica, ya que los ciberincidentes localizados podrían propagarse rápidamente desde cualquiera de las aproximadamente 22 000 entidades financieras de la Unión[28] a todo el sistema financiero, sin que los límites geográficos supongan un obstáculo. Los fallos de TIC graves en las finanzas no afectan únicamente a las entidades financieras de forma aislada. También allanan el camino para la propagación de vulnerabilidades localizadas a través de los canales de transmisión financieros y pueden provocar consecuencias adversas para la estabilidad del sistema financiero de la Unión, generando un pánico de liquidez y una pérdida general de confianza en los mercados financieros.

(4) En los últimos años, los riesgos de TIC han atraído la atención de los responsables políticos, reguladores y organismos de normalización nacionales, europeos e internacionales en un intento de aumentar la resiliencia, establecer normas y coordinar el trabajo de regulación o supervisión. A nivel internacional, el Comité de Supervisión Bancaria de Basilea, el Comité de Pagos e Infraestructuras del Mercado, el Consejo de Estabilidad Financiera, el Instituto de Estabilidad Financiera y los grupos de países del G-7 y el G-20 tienen por objeto proporcionar herramientas que refuercen la resiliencia de sus sistemas financieros a las autoridades competentes y a los operadores del mercado de diferentes países o territorios.

(5) A pesar de las iniciativas estratégicas y legislativas específicas nacionales y europeas, los riesgos de TIC siguen planteando un reto para la resiliencia operativa, el funcionamiento y la estabilidad del sistema financiero de la Unión. La reforma que siguió a la crisis financiera de 2008 reforzó principalmente la resiliencia financiera del sector financiero de la Unión y tenía por objeto salvaguardar la competitividad y la estabilidad de la Unión desde las perspectivas económica, prudencial y de conducta de mercado. Aunque la resiliencia digital y la seguridad de las TIC forman parte del riesgo operativo, el programa regulador posterior a la crisis se ha centrado menos en estas y solo se han desarrollado en algunos ámbitos de la política de servicios financieros y del panorama regulador de la Unión, o solo en unos pocos Estados miembros.

(6) El Plan de Acción en materia de Tecnología Financiera de 2018 de la Comisión[29] puso de relieve la importancia capital de hacer que el sector financiero de la Unión sea más

---

27 Informe de la JERS sobre el riesgo cibernético de febrero de 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

28 Según la evaluación de impacto que acompaña a la revisión de las Autoridades Europeas de Supervisión [SWD(2017) 308], existen alrededor de 5 665 entidades de crédito, 5 934 empresas de servicios de inversión, 2 666 empresas de seguros, 1 573 fondos de pensiones de empleo, 2 500 sociedades de gestión de inversiones, 350 infraestructuras de mercado (como entidades de contrapartida central, bolsas de valores, internalizadores sistemáticos, registros de operaciones y sistemas multilaterales de negociación), 45 agencias de calificación crediticia y 2 500 entidades de pago autorizadas y entidades de dinero electrónico. En total, unas 21 233 entidades sin incluir las sociedades de financiación participativa, los auditores legales y las sociedades de auditoría, los proveedores de servicios de criptoactivos y los administradores de índices de referencia.

29 Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Banco Central Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones, «Plan de acción en materia de tecnología financiera: por un sector financiero europeo más competitivo e innovador», COM(2018) 0109 final, https://ec.europa.eu/info/publications/180308-action-plan-fintech_en

resiliente también desde una perspectiva operativa para garantizar su seguridad tecnológica y su buen funcionamiento, así como su rápida recuperación de los incidentes y los fallos de los sistemas de TIC, permitiendo en última instancia que los servicios financieros se presten de manera eficaz y fluida en toda la Unión, incluso en situaciones de tensión, preservando al mismo tiempo la confianza de los consumidores y del mercado.

(7) En abril de 2019, la Autoridad Bancaria Europea (ABE), la Autoridad Europea de Valores y Mercados (AEVM) y la Autoridad Europea de Seguros y Pensiones de Jubilación (AESPJ) (denominadas conjuntamente «Autoridades Europeas de Supervisión» o «AES») emitieron conjuntamente dos dictámenes técnicos pidiendo un enfoque coherente del riesgo de TIC en las finanzas y recomendando reforzar, de manera proporcionada, la resiliencia operativa digital del sector de los servicios financieros a través de una iniciativa sectorial de la Unión.

(8) El sector financiero de la Unión está regulado por un código normativo único armonizado y cubierto por un sistema europeo de supervisión financiera. No obstante, las disposiciones que abordan la resiliencia operativa digital y la seguridad de las TIC aún no están plena o coherentemente armonizadas, a pesar de que la resiliencia operativa digital es vital para garantizar la estabilidad financiera y la integridad del mercado en la era digital, y no menos importante que, por ejemplo, las normas comunes prudenciales o de conducta de mercado. Por consiguiente, deben desarrollarse el código normativo único y el sistema de supervisión para abarcar también este componente, ampliando los mandatos de los supervisores financieros encargados de supervisar y proteger la estabilidad financiera y la integridad del mercado.

(9) Las disparidades legislativas y los enfoques reguladores o de supervisión nacionales desiguales del riesgo de TIC obstaculizan el mercado único de los servicios financieros, impidiendo el correcto ejercicio de la libertad de establecimiento y la prestación de servicios para las entidades financieras con presencia transfronteriza. La competencia entre el mismo tipo de entidades financieras que operan en diferentes Estados miembros también puede verse falseada. En particular, en ámbitos en los que la armonización de la Unión ha sido muy limitada (como las pruebas de resiliencia operativa digital) o inexistente (como el seguimiento del riesgo de terceros relacionado con las TIC), las disparidades derivadas de la evolución prevista a nivel nacional podrían generar nuevos obstáculos al funcionamiento del mercado único en detrimento de los participantes en el mercado y la estabilidad financiera.

(10) La forma parcial en que las disposiciones relacionadas con el riesgo de TIC se han abordado hasta ahora a escala de la Unión pone de manifiesto lagunas o solapamientos en ámbitos importantes, como la notificación de incidentes relacionados con las TIC y las pruebas de resiliencia operativa digital, y genera incoherencias debido a la aparición de normas nacionales divergentes o a la aplicación ineficaz en costes de normas que se solapan. Esto es especialmente perjudicial para los usuarios intensivos de las TIC, como el sector financiero, ya que los riesgos tecnológicos no tienen fronteras y el sector financiero despliega sus servicios a escala transfronteriza dentro y fuera de la Unión.

Las entidades financieras individuales que operan a escala transfronteriza o que poseen varias autorizaciones (por ejemplo, una entidad financiera puede tener sendas licencias de entidad bancaria, empresa de servicios de inversión y entidad de pago, cada una de ellas expedida por una autoridad competente diferente en uno o varios Estados

miembros) se enfrentan a retos operativos a la hora de abordar los riesgos de TIC y mitigar los efectos adversos de los incidentes de TIC por sí mismas y de manera coherente y eficaz en términos de costes.

(11) Dado que el código normativo único no ha ido acompañado de un marco global del riesgo operativo o de TIC, es necesaria una mayor armonización de los requisitos clave de resiliencia operativa digital para todas las entidades financieras. Las capacidades y la resiliencia general que las entidades financieras, sobre la base de estos requisitos clave, desarrollarían con vistas a hacer frente a las interrupciones operativas, contribuirían a preservar la estabilidad e integridad de los mercados financieros de la Unión y, de este modo, a garantizar un elevado nivel de protección de los inversores y consumidores de la Unión. Puesto que el objetivo del presente Reglamento es contribuir al buen funcionamiento del mercado único, debe basarse en las disposiciones del artículo 114 del TFUE, interpretado de conformidad con la jurisprudencia reiterada del Tribunal de Justicia de la Unión Europea.

(12) El presente Reglamento tiene por objeto, en primer lugar, consolidar y actualizar los requisitos relativos al riesgo de TIC abordados por separado hasta ahora en los diferentes Reglamentos y Directivas. Aunque esos actos jurídicos de la Unión cubrían las principales categorías de riesgo financiero (por ejemplo, riesgo de crédito, riesgo de mercado, riesgo de contraparte y riesgo de liquidez, riesgo de conducta de mercado), no pudieron abordar de manera exhaustiva, en el momento de su adopción, todos los componentes de la resiliencia operativa. Los requisitos en materia de riesgo operativo, cuando se desarrollaron más en estos actos jurídicos de la Unión, a menudo favorecieron un enfoque cuantitativo tradicional para abordar el riesgo (a saber, establecer un requisito de capital para cubrir los riesgos de TIC) en lugar de consagrar requisitos cualitativos específicos para impulsar las capacidades mediante requisitos orientados a las capacidades de protección, detección, contención, recuperación y reparación frente a incidentes relacionados con las TIC o mediante el establecimiento de capacidades de notificación y pruebas digitales. El objetivo principal de dichas Directivas y Reglamentos era recoger normas esenciales sobre supervisión prudencial, conducta o integridad del mercado.

Mediante este ejercicio, que consolida y actualiza las normas sobre el riesgo de TIC, todas las disposiciones que abordan el riesgo digital en las finanzas se reunirían por primera vez de manera coherente en un único acto legislativo. Así pues, esta iniciativa debe colmar las lagunas o subsanar incoherencias en algunos de esos actos jurídicos, también en relación con la terminología utilizada en ellos, y debe hacer referencia explícita al riesgo de TIC a través de normas específicas sobre las capacidades de gestión del riesgo de TIC, la presentación de informes, las pruebas y el seguimiento de los riesgos de terceros.

(13) Las entidades financieras deben seguir el mismo enfoque y las mismas normas basadas en principios a la hora de abordar el riesgo de TIC. La coherencia contribuye a aumentar la confianza en el sistema financiero y a preservar su estabilidad, especialmente en tiempos de uso excesivo de los sistemas, plataformas e infraestructuras de TIC, lo que conlleva un mayor riesgo digital.

El respeto de una ciberhigiene básica también debería evitar imponer costes elevados a la economía minimizando el impacto y los costes de las perturbaciones de las TIC.

(14) Utilizar un reglamento contribuye a reducir la complejidad normativa, fomenta la convergencia en materia de supervisión, aumenta la seguridad jurídica, al mismo tiempo que contribuye a limitar los costes de cumplimiento, especialmente para las

entidades financieras que operan a escala transfronteriza, y a reducir los falseamientos de la competencia. La elección de un reglamento para el establecimiento de un marco común para la resiliencia operativa digital de las entidades financieras parece, por tanto, la manera más adecuada de garantizar una aplicación homogénea y coherente de todos los componentes de la gestión del riesgo de TIC por parte de los sectores financieros de la Unión.

(15) Además de la legislación sobre servicios financieros, la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo[30] es el marco general actual de ciberseguridad a escala de la Unión. Entre los siete sectores críticos, dicha Directiva se aplica también a tres tipos de entidades financieras, a saber, las entidades de crédito, los centros de negociación y las entidades de contrapartida central. Sin embargo, dado que la Directiva (UE) 2016/1148 establece un mecanismo de identificación a nivel nacional de los operadores de servicios esenciales, solo determinadas entidades de crédito, centros de negociación y entidades de contrapartida central determinadas por los Estados miembros entran en su ámbito de aplicación y, por tanto, deben cumplir los requisitos de seguridad de TIC y notificación de incidentes establecidos en la misma.

(16) Dado que el presente Reglamento eleva el nivel de armonización de los componentes de resiliencia digital mediante la introducción de requisitos más estrictos en materia de gestión de riesgos de TIC y notificación de incidentes relacionados con las TIC con respecto a los establecidos en la legislación vigente de la Unión en materia de servicios financieros, ello constituye una mayor armonización también en comparación con los requisitos establecidos en la Directiva (UE) 2016/1148. Por consiguiente, el presente Reglamento constituye una *lex specialis* con respecto a la Directiva (UE) 2016/1148.

Es fundamental mantener una estrecha relación entre el sector financiero y el marco horizontal de ciberseguridad de la Unión, garantizando la coherencia con las estrategias de ciberseguridad ya adoptadas por los Estados miembros y permitiendo que los supervisores financieros tengan conocimiento de los ciberincidentes que afecten a otros sectores cubiertos por la Directiva (UE) 2016/1148.

(17) Para permitir un proceso de aprendizaje intersectorial y aprovechar eficazmente las experiencias de otros sectores a la hora de hacer frente a las ciberamenazas, las entidades financieras a que se refiere la Directiva (UE) 2016/1148 deben seguir formando parte del «ecosistema» de dicha Directiva (por ejemplo, el Grupo de Cooperación SRI y los CSIRT).

Las AES y las autoridades nacionales competentes deben poder participar en los debates estratégicos y en los trabajos técnicos, respectivamente, del Grupo de Cooperación SRI intercambiar información y seguir cooperando con los puntos de contacto únicos designados en virtud de la Directiva (UE) 2016/1148. Las autoridades competentes en virtud del presente Reglamento también deben consultar y cooperar con los CSIRT nacionales designados de conformidad con el artículo 9 de la Directiva (UE) 2016/1148.

(18) También es importante asegurar la coherencia con la Directiva sobre infraestructuras críticas europeas (ICE), que se está revisando actualmente para mejorar la protección y

[30] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (DO L 194 de 19.7.2016, p. 1).

la resiliencia de las infraestructuras críticas frente a las amenazas no cibernéticas, lo cual puede tener repercusiones en el sector financiero[31].

(19) Los proveedores de servicios de computación en nube son una categoría de proveedores de servicios digitales cubiertos por la Directiva (UE) 2016/1148. Como tales, están sujetos a una supervisión *ex post* llevada a cabo por las autoridades nacionales designadas con arreglo a dicha Directiva, que se limita a los requisitos de seguridad de TIC y notificación de incidentes establecidos en dicho acto. Dado que el marco de supervisión establecido por el presente Reglamento se aplica a todos los proveedores terceros esenciales de servicios de TIC, incluidos los proveedores de servicios de computación en nube, cuando presten servicios de TIC a entidades financieras, debe considerarse complementario de la supervisión que se está llevando a cabo en virtud de la Directiva (UE) 2016/1148. Además, el marco de supervisión establecido por el presente Reglamento debe abarcar a los proveedores de servicios de computación en nube en ausencia de un marco horizontal de la Unión aplicable a todos los sectores que establezca una autoridad de supervisión digital.

(20) Para mantener el pleno control de los riesgos de TIC, las entidades financieras necesitan disponer de capacidades globales que permitan una gestión de riesgos de TIC sólida y eficaz, junto con mecanismos y políticas específicos para la notificación de incidentes relacionados con las TIC, pruebas de sistemas, controles y procesos de TIC, así como para gestionar el riesgo de terceros relacionado con las TIC. Debe elevarse el umbral de resiliencia operativa digital para el sistema financiero, permitiendo al mismo tiempo una aplicación proporcionada de los requisitos para las entidades financieras que son microempresas, tal como se definen en la Recomendación 2003/361/CE de la Comisión[32].

(21) Los umbrales de notificación y las taxonomías de incidentes relacionados con las TIC varían considerablemente a nivel nacional. Si bien es cierto que se puede alcanzar una base común mediante la labor pertinente emprendida por la Agencia de la Unión Europea para la Ciberseguridad (ENISA)[33] y el Grupo de Cooperación en materia de SRI para las entidades financieras contempladas en la Directiva (UE) 2016/1148, todavía existen o pueden surgir enfoques divergentes sobre umbrales y taxonomías para el resto de entidades financieras. Esto implica múltiples requisitos a los que deben atenerse las entidades financieras, especialmente cuando operan en varios países de la Unión y cuando forman parte de un grupo financiero. Además, estas divergencias pueden obstaculizar la creación de nuevos mecanismos uniformes o centralizados de la Unión que aceleren el proceso de notificación y apoyen un intercambio rápido y fluido de información entre las autoridades competentes, lo cual es crucial para hacer frente a los riesgos de TIC en caso de ataques a gran escala con posibles consecuencias sistémicas.

---

31 Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección (DO L 345 de 23.12.2008, p. 75).

32 Recomendación de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas (DO L 124 de 20.5.2003, p. 36).

33 Taxonomía de la clasificación de incidentes de referencia de ENISA , https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy.

(22) Para que las autoridades competentes puedan desempeñar sus funciones de supervisión obteniendo una visión completa de la naturaleza, frecuencia, importancia e impacto de los incidentes relacionados con las TIC y a fin de mejorar el intercambio de información entre las autoridades públicas pertinentes, incluidas las autoridades policiales y judiciales y las autoridades de resolución, es necesario establecer normas para completar el régimen de notificación de incidentes relacionados con las TIC con los requisitos que actualmente faltan en la legislación de los subsectores financieros y eliminar los solapamientos y duplicaciones existentes para reducir los costes. Por lo tanto, es esencial armonizar el régimen de notificación de incidentes relacionados con las TIC, exigiendo a todas las entidades financieras que informen únicamente a sus autoridades competentes. Además, las AES deben estar facultadas para especificar en mayor medida los elementos de la notificación de incidentes relacionados con las TIC, como la taxonomía, los plazos, los conjuntos de datos, las plantillas y los umbrales aplicables.

(23) Los requisitos de las pruebas de resiliencia operativa digital se han desarrollado en algunos subsectores financieros dentro de varios marcos nacionales no coordinados que abordan los mismos problemas de manera diferente. Esto da lugar a la duplicación de costes para las entidades financieras transfronterizas y dificulta el reconocimiento mutuo de los resultados. Por lo tanto, las pruebas no coordinadas pueden segmentar el mercado único.

(24) Además, cuando no se requieren pruebas, no se detectan las vulnerabilidades, lo que supone un mayor riesgo para la entidad financiera y, en última instancia, para la estabilidad y la integridad del sector financiero. Sin la intervención de la Unión, las pruebas de resiliencia operativa digital seguirían siendo desiguales y no habría un reconocimiento mutuo de los resultados de las pruebas en diferentes países. Asimismo, dado que es poco probable que otros subsectores financieros adopten tales sistemas a una escala significativa, desaprovecharían las ventajas potenciales, como revelar vulnerabilidades y riesgos, poner a prueba las capacidades de defensa y la continuidad de las actividades, y aumentar la confianza de los clientes, los proveedores y los socios comerciales. Para poner remedio a tales solapamientos, divergencias y lagunas, es necesario establecer normas destinadas a que las entidades financieras y las autoridades competentes realicen pruebas coordinadas, facilitando así el reconocimiento mutuo de pruebas avanzadas para las entidades financieras significativas.

(25) La dependencia de los servicios de TIC por parte de las entidades financieras se debe en parte a su necesidad de adaptarse a una economía mundial digital competitiva emergente, de aumentar su eficiencia empresarial y de satisfacer la demanda de los consumidores. La naturaleza y el alcance de dicha dependencia han evolucionado continuamente en los últimos años, impulsando la reducción de costes en la intermediación financiera, permitiendo la expansión empresarial y la escalabilidad en el despliegue de actividades financieras, y ofreciendo al mismo tiempo una amplia gama de herramientas TIC para gestionar procesos internos complejos.

(26) Este amplio uso de los servicios de TIC se pone de manifiesto en acuerdos contractuales complejos, en los que las entidades financieras a menudo encuentran dificultades a la hora de negociar condiciones contractuales adaptadas a las normas prudenciales u otros requisitos reglamentarios a los que están sujetas, o a la hora de hacer valer derechos específicos, como los derechos de acceso o auditoría, cuando estos últimos están consagrados en los acuerdos. Además, muchos de estos contratos no ofrecen suficientes salvaguardias que permitan un control completo de los procesos

de subcontratación, privando así a la entidad financiera de su capacidad para evaluar estos riesgos asociados. Además, dado que los proveedores terceros de servicios de TIC a menudo prestan servicios normalizados a distintos tipos de clientes, tales contratos pueden no siempre satisfacer adecuadamente las necesidades individuales o específicas de los agentes del sector financiero.

(27) Aunque hay algunas normas generales sobre externalización en algunos actos legislativos de la Unión en materia de servicios financieros, el seguimiento de la dimensión contractual no está plenamente establecido en la legislación de la Unión. A falta de normas claras y específicas de la Unión aplicables a los acuerdos contractuales celebrados con los proveedores terceros de servicios de TIC, no se aborda de manera exhaustiva la fuente externa de riesgo de TIC. Por consiguiente, es necesario establecer determinados principios clave para orientar la gestión por parte de las entidades financieras del riesgo de terceros relacionado con las TIC, junto con un conjunto de derechos contractuales básicos en relación con varios elementos de la ejecución y rescisión de contratos, con vistas a consagrar determinadas salvaguardias mínimas que sustenten la capacidad de las entidades financieras de supervisar eficazmente todos los riesgos que se deriven de terceros proveedores de TIC.

(28) Hay una carencia de homogeneidad y convergencia en cuanto al riesgo de terceros relacionado con las TIC y a las dependencias de terceros en el sector de las TIC. A pesar de algunos esfuerzos para abordar el ámbito específico de la externalización, como las recomendaciones de 2017 sobre la externalización a proveedores de servicios en la nube[34], la cuestión del riesgo sistémico que puede desencadenar la exposición del sector financiero a un número limitado de proveedores terceros esenciales de servicios de TIC apenas se aborda en la legislación de la Unión. Esta carencia a nivel de la Unión se ve agravada por la ausencia de mandatos e instrumentos específicos que permitan a los supervisores nacionales adquirir una buena comprensión de las dependencias de terceros en el ámbito de las TIC y hacer un seguimiento adecuado de los riesgos derivados de la concentración de dichas dependencias de terceros en el ámbito de las TIC.

(29) Teniendo en cuenta los posibles riesgos sistémicos derivados del aumento de las prácticas de externalización y de la concentración de terceros en el sector de las TIC, y asimismo la insuficiencia de los mecanismos nacionales que permiten a los supervisores financieros cuantificar, calificar y corregir las consecuencias de los riesgos de TIC que se producen en proveedores terceros esenciales de servicios de TIC, es necesario establecer un marco de supervisión de la Unión adecuado que permita un seguimiento continuo de las actividades de los proveedores terceros de servicios de TIC que sean proveedores esenciales para las entidades financieras.

(30) Dado que las amenazas relacionadas con las TIC son cada vez más complejas y sofisticadas, las buenas medidas de detección y prevención dependen sustancialmente del intercambio periódico de información sobre amenazas y vulnerabilidades entre las entidades financieras. El intercambio de información contribuye a una mayor concienciación sobre las ciberamenazas, lo que, a su vez, mejora la capacidad de las entidades financieras para evitar que las amenazas se materialicen en incidentes reales y permite a las entidades financieras contener mejor los efectos de los incidentes relacionados con las TIC y recuperarse de manera más eficiente. A falta de

[34] Recomendaciones sobre la externalización a proveedores de servicios en la nube (EBA/REC/2017/03), ahora derogadas por las Directrices de la ABE sobre externalización (EBA/GL/2019/02).

orientaciones a escala de la Unión, varios factores parecen haber impedido este intercambio de información, en particular la incertidumbre sobre la compatibilidad con las normas de protección de datos, de defensa de la competencia y de responsabilidad.

(31) Además, las dudas sobre el tipo de información que puede compartirse con otros participantes en el mercado o con autoridades no supervisoras (como la ENISA, para información analítica, o Europol, con fines policiales) hacen que no se comparta información útil. El alcance y la calidad del intercambio de información sigue siendo limitado y fragmentado, ya que los intercambios pertinentes se realizan principalmente a nivel local (a través de iniciativas nacionales) y no existen mecanismos coherentes de intercambio de información a escala de la Unión adaptados a las necesidades de un sector financiero integrado.

(32) Por consiguiente, debe alentarse a las entidades financieras a aprovechar colectivamente sus conocimientos individuales y su experiencia práctica a nivel estratégico, táctico y operativo, con el fin de mejorar sus capacidades para evaluar y supervisar las ciberamenazas, defenderse de ellas y responder a las mismas, todo ello de forma adecuada. Por lo tanto, es necesario permitir la aparición a escala de la Unión de mecanismos de intercambio voluntario de información que, cuando se apliquen en entornos de confianza, ayuden a la comunidad financiera a prevenir y responder colectivamente a las amenazas, limitando rápidamente la propagación de los riesgos de TIC e impidiendo el posible contagio a través de los canales financieros. Estos mecanismos deben utilizarse respetando plenamente las normas de competencia de la Unión aplicables[35], así como de manera que se garantice el pleno respeto de las normas de la Unión en materia de protección de datos, principalmente el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo[36], en particular en el contexto del tratamiento de datos personales necesario para la satisfacción de los intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, tal como se contempla en el artículo 6, apartado 1, letra f), de dicho Reglamento.

(33) Sin perjuicio de la amplia cobertura prevista en el presente Reglamento, la aplicación de las normas de resiliencia operativa digital debe tener en cuenta las diferencias significativas entre entidades financieras en términos de tamaño, perfiles empresariales o exposición al riesgo digital. Como principio general, al destinar recursos y capacidades a la aplicación del marco de gestión de riesgos de TIC, las entidades financieras deben equilibrar debidamente sus necesidades relacionadas con las TIC con su tamaño y perfil empresarial, mientras que las autoridades competentes deben seguir evaluando y revisando el enfoque de dicha distribución.

(34) Dado que las entidades financieras de mayor tamaño pueden disponer de recursos más amplios y podrían movilizar rápidamente fondos para desarrollar estructuras de gobernanza y establecer diversas estrategias empresariales, solo las entidades financieras que no sean microempresas en el sentido del presente Reglamento deben estar obligadas a establecer mecanismos de gobernanza más complejos. Estas entidades están mejor equipadas, en particular, para establecer funciones de gestión

[35] Comunicación de la Comisión — Directrices sobre la aplicabilidad del artículo 101 del Tratado de Funcionamiento de la Unión Europea a los acuerdos de cooperación horizontal (DO C 11 de 14.1.2011, p. 1).

[36] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) (DO L 119 de 4.5.2016, p. 1).

específicas encaminadas a supervisar los acuerdos con proveedores terceros de servicios de TIC o a abordar la gestión de crisis, para organizar su gestión de riesgos de TIC con arreglo a las tres líneas del modelo de defensa, o para adoptar un documento de recursos humanos que explique exhaustivamente las políticas de derechos de acceso.

Del mismo modo, solo estas entidades financieras deben estar obligadas a llevar a cabo evaluaciones exhaustivas tras cambios importantes en los procesos y las infraestructuras de la red y los sistemas de información, a realizar periódicamente análisis de riesgos sobre los sistemas de TIC heredados, o a ampliar las pruebas efectuadas sobre los planes de continuidad de la actividad y de respuesta y recuperación para reflejar los escenarios de conmutación entre la infraestructura primaria de TIC y las instalaciones redundantes.

(35) Además, dado que solo las entidades financieras consideradas significativas a efectos de las pruebas avanzadas de resiliencia digital deben estar obligadas a llevar a cabo pruebas de penetración guiadas por amenazas, los procesos administrativos y los costes financieros derivados de la realización de dichas pruebas recaerían, en principio, en un pequeño porcentaje de entidades financieras. Por último, con el fin de aligerar la carga normativa, debe pedirse únicamente a las entidades financieras que no sean microempresas que informen periódicamente a las autoridades competentes de todos los costes y pérdidas causados por las perturbaciones de las TIC y de los resultados de las revisiones posteriores a los incidentes después de perturbaciones significativas de las TIC.

(36) Para garantizar la plena armonización y la coherencia general entre las estrategias empresariales de las entidades financieras, por una parte, y la gestión de riesgos de TIC, por otra, debe exigirse al órgano de dirección que desempeñe un papel central y activo en la dirección y adaptación del marco de gestión de riesgos de TIC y la estrategia global de resiliencia digital. El enfoque que adopte el órgano de dirección no solo debe centrarse en los medios para garantizar la resiliencia de los sistemas de TIC, sino que también debe abarcar a las personas y los procesos a través de un conjunto de políticas que promuevan, en cada nivel corporativo y para todo el personal, una fuerte concienciación sobre los riesgos cibernéticos y el compromiso de respetar una estricta ciberhigiene a todos los niveles.

La responsabilidad última del órgano de dirección en la gestión de los riesgos de TIC de una entidad financiera debe ser un principio fundamental de ese enfoque global, que se traducirá además en la implicación continua del órgano de dirección en el control del seguimiento de la gestión del riesgo de TIC.

(37) Además, la obligación del órgano de dirección de rendir plenamente cuentas va acompañada de la de garantizar un nivel de inversiones en TIC y un presupuesto global para que la entidad financiera pueda alcanzar su nivel de referencia en cuanto a la resiliencia operativa digital.

(38) Inspirándose en las pertinentes normas, directrices, recomendaciones o enfoques internacionales, nacionales y sectoriales en relación con la gestión del riesgo cibernético[37], el presente Reglamento promueve una serie de funciones que facilitan la

[37] CPIM-OICV, *Guidance on cyber resilience for financial market infrastructures* [«Orientaciones sobre la ciberresiliencia de las infraestructuras de los mercados financieros», documento en inglés], https://www.bis.org/cpmi/publ/d146.pdf G7, *Fundamental Elements of Cybersecurity for the Financial Sector,* [«Elementos fundamentales de la ciberseguridad para el sector financiero», documento en

estructuración general de la gestión del riesgo de TIC. Mientras las principales capacidades establecidas por las entidades financieras respondan a las necesidades de los objetivos previstos por las funciones (identificación, protección y prevención, detección, respuesta y recuperación, aprendizaje y evolución y comunicación) establecidas en el presente Reglamento, las entidades financieras seguirán teniendo libertad para utilizar modelos de gestión de riesgos de TIC que se enmarquen o categoricen de manera diferente.

(39) Para poder seguir haciendo frente a la naturaleza cambiante de las ciberamenazas, las entidades financieras deben mantener sistemas de TIC actualizados que sean fiables y estén dotados de la capacidad suficiente no solo para garantizar el tratamiento de datos necesario para la prestación de sus servicios, sino también para asegurar la resiliencia tecnológica que permita a las entidades financieras satisfacer adecuadamente las necesidades de tratamiento adicionales que un tensionamiento del mercado u otras situaciones adversas puedan generar. Aunque el presente Reglamento no implica ninguna normalización de sistemas, herramientas o tecnologías de TIC específicos, se basa en el uso adecuado por parte de las entidades financieras de las normas técnicas europeas e internacionalmente reconocidas (por ejemplo, ISO) o de las buenas prácticas del sector, en la medida en que dicho uso se ajuste plenamente a las instrucciones específicas de supervisión sobre el uso y la incorporación de normas internacionales.

(40) Se requieren planes eficientes de continuidad y recuperación de las actividades para que las entidades financieras puedan resolver pronta y rápidamente los incidentes relacionados con las TIC, en particular los ciberataques, limitando los daños y dando prioridad a la reanudación de las actividades y a las acciones de recuperación. No obstante, si bien los sistemas de copia de seguridad deben comenzar el tratamiento sin demoras indebidas, dicho inicio no debe en modo alguno poner en peligro la integridad y la seguridad de las redes y los sistemas de información ni la confidencialidad de los datos.

(41) Si bien el presente Reglamento permite a las entidades financieras determinar los objetivos de tiempo de recuperación de manera flexible y, por tanto, fijar tales objetivos teniendo plenamente en cuenta la naturaleza y el carácter esencial de la función pertinente y las necesidades comerciales específicas, al determinar dichos objetivos también debe exigirse una evaluación del posible impacto global en la eficiencia del mercado.

(42) Las consecuencias importantes de los ciberataques se amplifican cuando se producen en el sector financiero, un ámbito que corre mucho más riesgo de ser blanco de propagadores malintencionados que persiguen obtener beneficios financieros directamente en la fuente. Para mitigar tales riesgos y evitar que los sistemas de TIC pierdan integridad o dejen de estar disponibles, y que se vulneren datos confidenciales o que las infraestructuras físicas de TIC sufran daños, debe mejorarse significativamente la notificación de incidentes graves relacionados con las TIC por parte de las entidades financieras.

---

inglés] https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf; Marco de ciberseguridad del NIST, https://www.nist.gov/cyberframework; Herramientas de TICR del Consejo de Estabilidad Financiera, https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document

La notificación de incidentes relacionados con las TIC debe armonizarse para todas las entidades financieras exigiéndoles que informen únicamente a sus autoridades competentes. Aunque todas las entidades financieras estarían sujetas a esta notificación, no todas ellas deberían verse afectadas de la misma manera, ya que los umbrales de importancia relativa y los plazos pertinentes deben calibrarse para reflejar únicamente los incidentes graves relacionados con las TIC. La notificación directa permitiría a los supervisores financieros acceder a información sobre incidentes relacionados con las TIC. No obstante, los supervisores financieros deben transmitir esta información a las autoridades públicas no financieras (autoridades competentes en materia de SRI, autoridades nacionales de protección de datos y autoridades policiales o judiciales en caso de incidentes de carácter delictivo). La información sobre incidentes relacionados con las TIC debe canalizarse mutuamente: los supervisores financieros deben proporcionar a la entidad financiera todas las observaciones u orientaciones necesarias, mientras que las AES deben compartir datos anonimizados sobre amenazas y vulnerabilidades relacionadas con un determinado suceso para contribuir a una defensa colectiva más amplia.

(43) Debe preverse una mayor reflexión sobre la posible centralización de los informes de incidentes relacionados con las TIC a través de un único centro neurálgico de la UE que, bien reciba directamente los informes pertinentes y los notifique automáticamente a las autoridades nacionales competentes, bien centralice simplemente los informes transmitidos por las autoridades nacionales competentes y desempeñe una función de coordinación. Debe exigirse a las AES que, consultando con el BCE y la ENISA y antes de una fecha determinada, elaboren un informe conjunto en el que se estudie la viabilidad de crear dicho centro neurálgico de la UE.

(44) Con el fin de lograr una sólida resiliencia operativa digital, y en consonancia con las normas internacionales (por ejemplo, los Elementos Fundamentales del G7 para las pruebas de penetración guiadas por amenazas), las entidades financieras deben probar periódicamente su personal y sus sistemas de TIC con respecto a la efectividad de sus capacidades de prevención, detección, respuesta y recuperación, a fin de descubrir y abordar posibles vulnerabilidades de TIC. Para responder a las diferencias entre los subsectores financieros y dentro de ellos en relación con la preparación de las entidades financieras en materia de ciberseguridad, las pruebas deben incluir una amplia variedad de herramientas y acciones, que van desde una evaluación de los requisitos básicos (por ejemplo, evaluaciones y exploraciones de vulnerabilidad, análisis del código abierto, evaluaciones de la seguridad de la red, análisis de carencias, revisiones de seguridad física, cuestionarios y soluciones de software de exploración, revisiones del código fuente cuando sea posible, pruebas basadas en escenarios, pruebas de compatibilidad, pruebas de rendimiento o pruebas de extremo a extremo) hasta pruebas más avanzadas (por ejemplo, pruebas de penetración guiadas por amenazas en el caso de las entidades financieras suficientemente maduras desde la perspectiva de las TIC para realizar estas pruebas). Las pruebas de resiliencia operativa digital deberían, por tanto, ser más exigentes para las entidades financieras significativas (como grandes entidades de crédito, bolsas de valores, depositarios centrales de valores, entidades de contrapartida central, etc.). Al mismo tiempo, las pruebas de resiliencia operativa digital también deberían ser más relevantes para algunos subsectores que desempeñan un papel sistémico fundamental (por ejemplo, pagos, banca, compensación y liquidación) y menos relevantes para otros subsectores (por ejemplo, gestores de activos, agencias de calificación crediticia, etc.). Las entidades financieras transfronterizas que ejerzan su libertad de establecimiento o prestación de servicios en la Unión deben cumplir un único conjunto de requisitos de

pruebas avanzadas (por ejemplo, pruebas de penetración guiadas por amenazas) en su Estado miembro de origen, y dicha prueba debe incluir las infraestructuras de TIC en todos los países o territorios en los que el grupo transfronterizo opere dentro de la Unión, permitiendo así que los grupos transfronterizos solo incurran en costes de pruebas en un país.

(45) Para garantizar un seguimiento sólido del riesgo de terceros relacionado con las TIC, es necesario establecer un conjunto de normas basadas en principios para orientar el seguimiento por parte de las entidades financieras de los riesgos que surgen en el contexto de las funciones externalizadas a proveedores terceros de servicios de TIC y, de manera más general, en el contexto de las dependencias de terceros relacionadas con las TIC.

(46) Una entidad financiera debe seguir siendo en todo momento plenamente responsable del cumplimiento de las obligaciones derivadas del presente Reglamento. Debe organizarse un seguimiento proporcionado de los riesgos que surjan a nivel del proveedor tercero de servicios de TIC teniendo debidamente en cuenta la escala, complejidad e importancia de las dependencias relacionadas con las TIC, el carácter esencial o la importancia de los servicios, procesos o funciones sujetos a los acuerdos contractuales y, en última instancia, sobre la base de una evaluación cuidadosa de cualquier posible impacto en la continuidad y calidad de los servicios financieros a nivel individual y de grupo, según proceda.

(47) La realización de dicho seguimiento debe seguir un enfoque estratégico para el riesgo de terceros relacionado con las TIC formalizado mediante la adopción por parte del órgano de dirección de la entidad financiera de una estrategia específica, basada en un examen continuo de todas esas dependencias de terceros relacionadas con las TIC. Para aumentar la sensibilización en de los supervisores sobre las dependencias de terceros en el sector de las TIC, y con vistas a apoyar en mayor medida el marco de supervisión establecido por el presente Reglamento, los supervisores financieros deben recibir periódicamente información esencial de los registros y deben poder solicitar extractos de la misma sobre una base *ad hoc*.

(48) Un análisis exhaustivo previo a la contratación debe sustentar y preceder a la celebración formal de acuerdos contractuales, mientras que la rescisión de los contratos debe estar motivada, como mínimo, por una serie de circunstancias que pongan de manifiesto deficiencias en el proveedor tercero de servicios de TIC.

(49) Para abordar el impacto sistémico del riesgo de concentración de terceros en el ámbito de las TIC, debe promoverse una solución equilibrada mediante un enfoque flexible y gradual, ya que unos techos rígidos o unas limitaciones estrictas pueden obstaculizar la conducta empresarial y la libertad contractual. Las entidades financieras deben evaluar exhaustivamente los acuerdos contractuales para determinar la probabilidad de que aparezca dicho riesgo, incluso mediante análisis en profundidad de los acuerdos de subexternalización, en particular cuando se celebren con proveedores terceros de servicios de TIC establecidos en un tercer país. En esta fase, y con el fin de lograr un equilibrio justo entre el imperativo de preservar la libertad contractual y el de garantizar la estabilidad financiera, no se considera apropiado establecer techos y límites estrictos a las exposiciones frente a terceros en el ámbito de las TIC. En el ejercicio de las tareas de supervisión, la AES designada para llevar a cabo la supervisión de cada proveedor tercero esencial de TIC («el supervisor principal») debe prestar especial atención a comprender plenamente la magnitud de las interdependencias y descubrir los casos específicos en los que un alto grado de

concentración de proveedores terceros esenciales de servicios de TIC en la Unión pueda poner bajo presión la estabilidad e integridad del sistema financiero de la Unión, y debe, en su lugar, facilitar un diálogo con los proveedores terceros esenciales de servicios de TIC cuando se detecte ese riesgo[38].

(50) Para poder evaluar y controlar periódicamente la capacidad del proveedor tercero de servicios de TIC para prestar servicios de forma segura a la entidad financiera sin que ello afecte negativamente a la capacidad de resiliencia de esta, debe existir una armonización de los elementos contractuales clave a lo largo de la ejecución de los contratos con proveedores terceros de TIC. Estos elementos solo cubren aspectos contractuales mínimos que se consideran cruciales para permitir un seguimiento completo por parte de la entidad financiera con vistas a garantizar su resiliencia digital, que depende de la estabilidad y la seguridad del servicio de TIC.

(51) Los acuerdos contractuales deben prever, en particular, descripciones completas de las funciones y servicios, de los lugares en los que se prestan tales funciones y en los que se procesan los datos, así como descripciones completas del nivel de servicio, acompañadas de objetivos de rendimiento cuantitativos y cualitativos dentro de los niveles de servicio acordados, a fin de permitir un seguimiento eficaz por parte de la entidad financiera. En la misma línea, las disposiciones sobre accesibilidad, disponibilidad, integridad, seguridad y protección de los datos personales, así como las garantías de acceso, recuperación y devolución en caso de insolvencia, resolución o interrupción de las operaciones comerciales del proveedor tercero de servicios de TIC también deben considerarse elementos esenciales para la capacidad de una entidad financiera de garantizar el control del riesgo de terceros.

(52) Para garantizar que las entidades financieras mantengan el pleno control de todos los cambios que puedan afectar a su seguridad de TIC, deben establecerse plazos de notificación y obligaciones de información del proveedor tercero de servicios de TIC en caso de cambios que puedan tener un impacto importante en la capacidad del proveedor tercero de servicios de TIC para desempeñar eficazmente funciones esenciales o importantes, incluida la prestación de asistencia por parte de este último en caso de incidente relacionado con las TIC sin coste adicional o a un coste determinado de antemano.

(53) Los derechos de acceso, inspección y auditoría por parte de la entidad financiera o de un tercero designado son instrumentos cruciales en el seguimiento permanente por parte de las entidades financieras del rendimiento del proveedor tercero de servicios de TIC, junto con la plena cooperación de este último durante las inspecciones. En la misma línea, la autoridad competente de la entidad financiera debe tener el derecho de inspeccionar y auditar, previa notificación, al proveedor tercero de servicios de TIC, sin perjuicio de la confidencialidad.

(54) Los acuerdos contractuales deben prever derechos de rescisión claros y los correspondientes preavisos mínimos, así como estrategias específicas de salida que permitan, en particular, períodos transitorios obligatorios durante los cuales los proveedores terceros de servicios de TIC deben seguir desempeñando las funciones pertinentes con vistas a reducir el riesgo de perturbaciones a nivel de la entidad

[38] Además, en caso de que surja el riesgo de abuso por parte de un proveedor tercero de servicios de TIC que se considere dominante, las entidades financieras también deben tener la posibilidad de presentar una denuncia formal o informal ante la Comisión Europea o ante las autoridades nacionales de defensa de la competencia.

financiera, o permitir a esta última recurrir efectivamente a otros proveedores terceros de servicios de TIC, o alternativamente a soluciones internas, en consonancia con la complejidad del servicio prestado.

(55) Además, el uso voluntario de las cláusulas contractuales tipo desarrolladas por la Comisión para los servicios de computación en la nube puede ofrecer mayor confianza a las entidades financieras y a sus proveedores terceros de TIC, al aumentar el nivel de seguridad jurídica sobre el uso de los servicios de computación en la nube por parte del sector financiero, respetando plenamente los requisitos y expectativas establecidos en la normativa sobre servicios financieros. Ese trabajo se basa en las medidas ya previstas en el Plan de Acción en materia de Tecnología Financiera de 2018, que anunciaba la intención de la Comisión de fomentar y facilitar el desarrollo de cláusulas contractuales tipo para la externalización de servicios de computación en la nube por parte de las entidades financieras, basándose en los esfuerzos intersectoriales de las partes interesadas del ámbito de los servicios de computación en la nube, que la Comisión ha facilitado con la ayuda de la participación del sector financiero.

(56) Los proveedores terceros esenciales de servicios de TIC deben estar sujetos a un marco de supervisión de la Unión, con vistas a promover la convergencia y la eficiencia en relación con los enfoques de supervisión del riesgo de terceros relacionado con las TIC en el sector financiero, reforzar la resiliencia operativa digital de las entidades financieras que dependen de proveedores terceros esenciales de servicios de TIC para el desempeño de funciones operativas, y contribuir así a preservar la estabilidad del sistema financiero de la Unión y la integridad del mercado único de servicios financieros.

(57) Dado que solo los proveedores terceros esenciales de servicios requieren un trato especial, debe establecerse un mecanismo de designación a efectos de la aplicación del marco de supervisión de la Unión para tener en cuenta la dimensión y la naturaleza de la dependencia del sector financiero de dichos proveedores terceros de servicios de TIC, consistente en un conjunto de criterios cuantitativos y cualitativos que establecerían los parámetros para determinar el carácter esencial a efectos de la inclusión en la supervisión. Los proveedores terceros esenciales de servicios de TIC que no sean designados automáticamente en virtud de la aplicación de los criterios mencionados anteriormente deben tener la posibilidad de participar voluntariamente en el marco de supervisión, mientras que los proveedores terceros de TIC que ya estén sujetos a los mecanismos de vigilancia establecidos a nivel del Eurosistema con el fin de apoyar las funciones a que se refiere el artículo 127, apartado 2, del Tratado de Funcionamiento de la Unión Europea deben quedar exentos.

(58) El requisito de la constitución legal en la Unión de los proveedores terceros de servicios de TIC que hayan sido designados como esenciales no equivale a un requisito de localización de datos, ya que el presente Reglamento no contiene ninguna otra exigencia de que el almacenamiento o tratamiento de datos deba llevarse a cabo en la Unión.

(59) Este marco debe entenderse sin perjuicio de la competencia de los Estados miembros para llevar a cabo sus propias misiones de supervisión con respecto a los proveedores terceros de servicios de TIC que no sean esenciales en virtud del presente Reglamento, pero que podrían considerarse importantes a nivel nacional.

(60) Para aprovechar la actual arquitectura institucional de múltiples niveles en el ámbito de los servicios financieros, el Comité Mixto de las AES debe seguir garantizando la coordinación intersectorial general en relación con todos los asuntos relacionados con

el riesgo de TIC, de conformidad con sus funciones en materia de ciberseguridad, con el apoyo de un nuevo Subcomité (el Foro de Supervisión) que lleve a cabo trabajos preparatorios tanto para decisiones individuales dirigidas a proveedores terceros esenciales de servicios de TIC como para recomendaciones colectivas, en particular sobre la evaluación comparativa de los programas de supervisión de proveedores terceros esenciales de servicios de TIC, y que determine las buenas prácticas para abordar las cuestiones relativas al riesgo de concentración de TIC.

(61) A fin de garantizar que los proveedores terceros de servicios de TIC que desempeñen un papel esencial en el funcionamiento del sector financiero sean objeto de una supervisión proporcionada a escala de la Unión, debe designarse a una de las AES como supervisor principal para cada proveedor tercero esencial de servicios de TIC.

(62) Los supervisores principales deben gozar de las competencias necesarias para llevar a cabo investigaciones e inspecciones *in situ* y a distancia de proveedores terceros esenciales de servicios de TIC, acceder a todos los locales y lugares pertinentes y obtener información completa y actualizada que les permita contar con una visión real del tipo, dimensión e impacto del riesgo de terceros relacionado con las TIC a que se enfrentan las entidades financieras y, en última instancia, el sistema financiero de la Unión.

Encomendar a las AES la supervisión principal es un requisito previo para captar y abordar la dimensión sistémica del riesgo de TIC en las finanzas. El lugar que ocupan en la Unión los proveedores terceros esenciales de servicios de TIC y los consiguientes problemas potenciales del riesgo de concentración de TIC exigen adoptar un enfoque colectivo aplicado a nivel de la Unión. El ejercicio de múltiples derechos de auditoría y acceso, llevado a cabo por numerosas autoridades competentes por separado y con una coordinación escasa o nula, no daría lugar a una visión general completa del riesgo de terceros relacionado con las TIC, al tiempo que crearía redundancias, cargas y complejidad innecesarias para los proveedores terceros esenciales de TIC sobre los que recaigan tales solicitudes.

(63) Además, los supervisores principales deben poder presentar recomendaciones sobre cuestiones relacionadas con el riesgo de TIC y soluciones adecuadas, oponiéndose asimismo a determinados acuerdos contractuales que afecten en última instancia a la estabilidad de la entidad financiera o del sistema financiero. El cumplimiento de dichas recomendaciones sustantivas establecidas por los supervisores principales debe ser tenido debidamente en cuenta por las autoridades nacionales competentes en el marco de su función de supervisión prudencial de las entidades financieras.

(64) El marco de supervisión no sustituirá, ni en modo alguno ni en ninguna parte, a la gestión por las entidades financieras del riesgo que entraña el recurso a proveedores terceros de servicios de TIC, incluida la obligación de hacer un seguimiento permanente de sus acuerdos contractuales celebrados con proveedores terceros esenciales de servicios de TIC, y no afectará a la plena responsabilidad de las entidades financieras en el cumplimiento y la observancia de todos los requisitos del presente Reglamento y de la legislación pertinente en materia de servicios financieros. Para evitar duplicaciones y solapamientos, las autoridades competentes deben abstenerse de adoptar individualmente cualquier medida destinada a supervisar los riesgos de los proveedores terceros esenciales de servicios de TIC. Estas medidas deben coordinarse y acordarse previamente en el contexto del marco de supervisión.

(65) A fin de promover la convergencia a nivel internacional sobre las buenas prácticas que deben utilizarse en la revisión de la gestión de riesgos digitales por parte de

proveedores terceros de servicios de TIC, debe alentarse a las AES a que celebren acuerdos de cooperación con las autoridades competentes pertinentes de terceros países en materia de supervisión y regulación, a fin de facilitar el desarrollo de buenas prácticas que aborden el riesgo de terceros relacionado con las TIC.

(66) Para aprovechar la pericia técnica de los expertos de las autoridades competentes en gestión de riesgos operativos y de TIC, los supervisores principales deben basarse en la experiencia nacional en materia de supervisión y crear equipos de examen específicos para cada proveedor tercero esencial de servicios de TIC, agrupando equipos multidisciplinares para apoyar tanto la preparación como la ejecución real de las actividades de supervisión, incluidas las inspecciones *in situ* de proveedores terceros esenciales de servicios de TIC, así como el seguimiento necesario de las mismas.

(67) Las autoridades competentes deben disponer de todas las facultades de supervisión, investigación y sanción necesarias para garantizar la aplicación del presente Reglamento. En principio, las sanciones administrativas deben hacerse públicas. Dado que las entidades financieras y los proveedores terceros de servicios de TIC pueden estar establecidos en diferentes Estados miembros y estar bajo la supervisión de diferentes autoridades sectoriales competentes, se debe garantizar una estrecha cooperación entre las pertinentes autoridades competentes, incluido el BCE, en relación con las tareas específicas que le encomienda el Reglamento (UE) n.º 1024/2013 del Consejo[39], y debe garantizarse la consulta con las AES mediante el intercambio de información y la prestación de asistencia mutua en el contexto de las actividades de supervisión.

(68) A fin de cuantificar y calificar en mayor medida los criterios de designación de proveedores terceros esenciales de servicios de TIC y armonizar las tasas de supervisión, deben delegarse en la Comisión los poderes para adoptar actos con arreglo al artículo 290 del Tratado de Funcionamiento de la Unión Europea encaminados a especificar con más detalle: el impacto sistémico que un fallo de un proveedor tercero de TIC podría tener en las entidades financieras a las que presta servicios, el número de entidades de importancia sistémica mundial (EISM) u otras entidades de importancia sistémica (OEIS) que dependen del proveedor tercero de servicios de TIC correspondiente, el número de proveedores terceros de servicios de TIC activos en un mercado específico, los costes de migración a otro proveedor tercero de servicios de TIC, el número de Estados miembros en los que el proveedor tercero de servicios de TIC pertinente presta servicios y en los que las entidades financieras que recurren a sus servicios operan, así como la cuantía de las tasas de supervisión y las modalidades de pago.

Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante la labor preparatoria, en particular con expertos, y que esas consultas se realicen de conformidad con los principios establecidos en el Acuerdo interinstitucional de 13 de abril de 2016 sobre la mejora de la legislación[40]. En particular, a fin de garantizar una participación equitativa en la preparación de los actos delegados, el Parlamento Europeo y el Consejo reciben toda la documentación al

[39] Reglamento (UE) n.° 1024/2013 del Consejo, de 15 de octubre de 2013, que encomienda al Banco Central Europeo tareas específicas respecto de políticas relacionadas con la supervisión prudencial de las entidades de crédito (DO L 287 de 29.10.2013, p. 63).

[40] DO L 123 de 12.5.2016, p. 1.

mismo tiempo que los expertos de los Estados miembros, y sus expertos tienen acceso sistemáticamente a las reuniones de los grupos de expertos de la Comisión que se ocupen de la preparación de actos delegados.

(69) Dado que el presente Reglamento, junto con la Directiva (UE) 20xx/xx del Parlamento Europeo y del Consejo[41], implica una consolidación de las disposiciones en materia de gestión del riesgo de TIC que se extienden por múltiples reglamentos y directivas del acervo de la Unión en materia de servicios financieros, incluidos los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014 y (UE) n.º 909/2014, y con el fin de garantizar la plena coherencia, dichos Reglamentos deben modificarse para aclarar que las disposiciones pertinentes relacionadas con el riesgo de TIC se establecen en el presente Reglamento.

Debe garantizarse la armonización coherente de los requisitos establecidos en el presente Reglamento mediante normas técnicas. Como organismos que disponen de conocimientos técnicos altamente especializados, debe otorgarse a las AES el mandato de elaborar proyectos de normas técnicas de regulación que no conlleven opciones políticas, para su presentación a la Comisión. Deben elaborarse normas técnicas de regulación en los ámbitos de la gestión del riesgo de TIC, la presentación de información, las pruebas y los requisitos clave para un seguimiento sólido del riesgo de terceros relacionado con las TIC.

(70) Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos. La Comisión y las AES deben velar por que todas las entidades financieras puedan aplicar esas normas y esos requisitos de manera proporcionada a la naturaleza, la escala y la complejidad de dichas entidades y de sus actividades.

(71) Para facilitar la comparabilidad de los informes sobre incidentes graves relacionados con las TIC y garantizar la transparencia de los acuerdos contractuales para el uso de servicios de TIC prestados por proveedores terceros de servicios de TIC, debe encomendarse a las AES la elaboración de proyectos de normas técnicas de ejecución que establezcan plantillas, formularios y procedimientos normalizados para que las entidades financieras notifiquen un incidente grave relacionado con las TIC, así como plantillas normalizadas para el registro de información. A la hora de elaborar dichas normas, las AES deben tener en cuenta el tamaño y la complejidad de las entidades financieras, así como la naturaleza y el nivel de riesgo de sus actividades. Se deben otorgar a la Comisión competencias para adoptar dichas normas técnicas de ejecución mediante actos de ejecución, con arreglo al artículo 291 del TFUE y de conformidad con el artículo 15 de los Reglamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 y (UE) n.º 1095/2010. Dado que ya se han especificado requisitos adicionales mediante actos delegados y de ejecución basados en normas técnicas de regulación y de ejecución previstas en los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014 y (UE) n.º 909/2014, procede encargar a las AES, ya sea individual o conjuntamente a través del Comité Mixto, que presenten a la Comisión normas técnicas de regulación y de ejecución para la adopción de actos delegados y de ejecución que recojan y actualicen las actuales normas de gestión del riesgo de TIC.

(72) Este ejercicio implicará la consiguiente modificación de los actos delegados y de ejecución vigentes adoptados en diferentes ámbitos de la legislación sobre servicios financieros. El ámbito de aplicación de los artículos sobre el riesgo operativo en virtud

[41] [*Insértese la referencia completa*]

de los cuales las habilitaciones contenidas en dichos actos preveían la adopción de actos delegados y de ejecución debe modificarse con el fin de incorporar al presente Reglamento todas las disposiciones relativas a la resiliencia operativa digital que forman actualmente parte de dichos Reglamentos.

(73) Dado que los objetivos del presente Reglamento, a saber, conseguir un alto nivel de resiliencia operativa digital aplicable a todas las entidades financieras, no pueden alcanzarse de manera suficiente por los Estados miembros, pues requieren la armonización de una multitud de normas diferentes, que en la actualidad existen, bien en determinados actos de la Unión, bien en los ordenamientos jurídicos de los distintos Estados miembros, sino que, debido a sus dimensiones y efectos, pueden lograrse mejor a escala de la Unión, esta última puede adoptar medidas de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad establecido en el mismo artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo.

HAN ADOPTADO EL PRESENTE REGLAMENTO:

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1

Objeto

1. El presente Reglamento establece requisitos uniformes relativos a la seguridad de las redes y los sistemas de información que sustentan los procesos empresariales de las entidades financieras, los cuales son necesarios para lograr un elevado nivel común de resiliencia operativa digital y comprenden lo siguiente:

   (a) requisitos aplicables a las entidades financieras en relación con:

   – la gestión de riesgos en el ámbito de las tecnologías de la información y la comunicación (TIC);

   – la notificación de incidentes graves relacionados con las TIC a las autoridades competentes;

   – las pruebas de resiliencia operativa digital;

   – el intercambio de información e inteligencia en relación con las ciberamenazas y las vulnerabilidades cibernéticas;

   – las medidas para una buena gestión por parte de las entidades financieras del riesgo de terceros relacionado con las TIC;

   (b) requisitos en relación con los acuerdos contractuales celebrados entre proveedores terceros de servicios de TIC y entidades financieras;

   (c) el marco de supervisión de los proveedores terceros esenciales de servicios de TIC cuando presten servicios a entidades financieras;

   (d) normas sobre cooperación entre autoridades competentes y normas sobre supervisión y ejecución por parte de las autoridades competentes en relación con todos los asuntos cubiertos por el presente Reglamento.

2. En relación con las entidades financieras identificadas como operadores de servicios esenciales con arreglo a las normas nacionales que transponen el artículo 5 de la Directiva (UE) 2016/1148, el presente Reglamento se considerará un acto jurídico sectorial de la Unión a efectos del artículo 1, apartado 7, de dicha Directiva.

Artículo 2

Ámbito de aplicación personal

1. El presente Reglamento se aplicará a las siguientes entidades:

   (a) entidades de crédito,

   (b) entidades de pago,

   (c) entidades de dinero electrónico,

   (d) empresas de servicios de inversión,

   (e) proveedores de servicios de criptoactivos, emisores de criptoactivos, emisores de fichas referenciadas a activos y emisores de fichas significativas referenciadas a activos,

   (f) depositarios centrales de valores,

   (g) entidades de contrapartida central,

   (h) centros de negociación,

   (i) registros de operaciones,

   (j) gestores de fondos de inversión alternativos,

   (k) sociedades de gestión,

   (l) proveedores de servicios de suministro de datos,

   (m) empresas de seguros y de reaseguros,

   (n) intermediarios de seguros, intermediarios de reaseguros e intermediarios de seguros complementarios,

   (o) fondos de pensiones de jubilación,

   (p) agencias de calificación crediticia,

   (q) auditores legales y sociedades de auditoría,

   (r) administradores de índices de referencia cruciales,

   (s) proveedores de servicios de financiación participativa,

   (t) registros de titulizaciones,

   (u) proveedores terceros de servicios de TIC.

2. A efectos del presente Reglamento, las entidades a que se refieren las letras a) a t) se denominarán colectivamente «entidades financieras».

Artículo 3

Definiciones

A efectos del presente Reglamento, se entenderá por:

(1) «resiliencia operativa digital»: la capacidad de una entidad financiera para construir, garantizar y revisar su integridad operativa desde una perspectiva tecnológica garantizando, directa o indirectamente, mediante el uso de servicios de proveedores terceros de TIC, toda la gama de capacidades relacionadas con las TIC necesarias para preservar la seguridad de las redes y los sistemas de información de los que haga uso una entidad financiera y que sustenten la prestación continuada de servicios financieros y su calidad;

(2) «redes y sistemas de información»: las redes y los sistemas de información según se definen en el artículo 4, punto 1, de la Directiva (UE) 2016/1148;

(3) «seguridad de las redes y los sistemas de información»: la seguridad de las redes y los sistemas de información según se definen en el artículo 4, punto 2, de la Directiva (UE) 2016/1148;

(4) «riesgo de TIC»: cualquier circunstancia razonablemente identificable en relación con el uso de redes y sistemas de información, incluidos un mal funcionamiento, un rebasamiento de capacidad, un fallo, una perturbación, un deterioro, un uso indebido, una pérdida u otro tipo de suceso malintencionado o no malintencionado, que, si se materializa, puede comprometer la seguridad de las redes y los sistemas de información, de cualquier herramienta o proceso dependiente de la tecnología, de la ejecución de las operaciones y los procesos, o de la prestación de servicios, poniendo así en peligro la integridad o la disponibilidad de los datos, el software o cualquier otro componente de los servicios e infraestructuras de TIC, u ocasionando una vulneración de la confidencialidad, daños a la infraestructura física de las TIC u otros efectos adversos;

(5) «activo de información»: un compendio de información, tangible o intangible, que conviene proteger;

(6) «incidente relacionado con las TIC»: un suceso no previsto detectado en las redes y los sistemas de información, debido o no a una actividad malintencionada, que ponga en peligro la seguridad de las redes y sistemas de información, de la información que procesan, almacenan o transmiten dichos sistemas, o que tenga efectos adversos sobre la disponibilidad, confidencialidad, continuidad o autenticidad de los servicios financieros prestados por la entidad financiera;

(7) «incidente grave relacionado con las TIC»: un incidente relacionado con las TIC con un impacto adverso potencialmente elevado en las redes y los sistemas de información que sustentan las funciones esenciales de la entidad financiera;

(8) «ciberamenaza»: una ciberamenaza tal como se define en el artículo 2, punto 8, del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo[42];

(9) «ciberataque»: un incidente malintencionado relacionado con las TIC consistente en un intento de destruir, exponer, alterar, desactivar o robar un activo, obtener acceso no autorizado a ese activo o hacer uso no autorizado del mismo, perpetrado por cualquier actor de amenazas;

[42] Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad») (DO L 151 de 7.6.2019, p. 15).

(10) «inteligencia sobre amenazas»: información que se ha agregado, transformado, analizado, interpretado o enriquecido para proporcionar el contexto necesario para la toma de decisiones y que aporta una comprensión pertinente y suficiente para mitigar el impacto de un incidente relacionado con las TIC o una ciberamenaza, incluidos los detalles técnicos de un ciberataque, los responsables del ataque, su *modus operandi* y sus motivaciones;

(11) «defensa en profundidad»: estrategia relacionada con las TIC que integra a las personas, los procesos y la tecnología para establecer una variedad de barreras en múltiples capas y dimensiones de la entidad;

(12) «vulnerabilidad»: debilidad, susceptibilidad o defecto de un activo, sistema, proceso o control que puede ser explotado por una amenaza;

(13) «pruebas de penetración guiadas por amenazas»: un marco que imita las tácticas, técnicas y procedimientos de actores de amenazas reales que se considera presentan una auténtica ciberamenaza, y que da lugar a una prueba controlada, a medida y basada en inteligencia (equipo rojo) de los sistemas de producción en vivo esenciales de la entidad;

(14) «riesgo de terceros relacionado con las TIC»: el riesgo de TIC que puede surgir para una entidad financiera en relación con su uso de servicios de TIC prestados por proveedores terceros de servicios de TIC o por subcontratistas de estos últimos;

(15) «proveedor tercero de servicios de TIC»: una empresa que presta servicios digitales y de datos, incluidos los proveedores de servicios de computación en la nube, software, servicios de análisis de datos y centros de datos, pero excluidos los proveedores de componentes de hardware y las empresas autorizadas con arreglo al Derecho de la Unión que prestan servicios de comunicaciones electrónicas, tal como se definen en el artículo 2, punto 4, de la Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo[43];

(16) «servicios de TIC»: servicios digitales y de datos prestados a través de los sistemas de TIC a uno o varios usuarios internos o externos, incluidos los servicios de suministro de datos, introducción de datos, almacenamiento de datos, tratamiento y comunicación de datos, la comprobación de datos y los servicios de apoyo a las empresas y a la toma de decisiones basados en datos;

(17) «función esencial o importante»: una función cuya interrupción o ejecución defectuosa o fallida afectaría significativamente al cumplimiento continuado de una entidad financiera con las condiciones y obligaciones de su autorización, o con sus demás obligaciones en virtud de la legislación aplicable en materia de servicios financieros, o a su rendimiento financiero o a la solidez o continuidad de sus servicios y actividades;

(18) «proveedor tercero esencial de servicios de TIC»: un proveedor tercero de servicios de TIC designado de conformidad con el artículo 29 y sujeto al marco de supervisión a que se refieren los artículos 30 a 37;

(19) «proveedor tercero de servicios de TIC establecido en un tercer país»: un proveedor tercero de servicios de TIC que sea una persona jurídica establecida en un tercer país,

[43] Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas (refundición) (DO L 321 de 17.12.2018, p. 36).

no se haya instalado ni esté presente en la Unión y haya celebrado un acuerdo contractual con una entidad financiera para la prestación de servicios de TIC;

(20) «subcontratista de TIC establecido en un tercer país»: un subcontratista de TIC que sea una persona jurídica establecida en un tercer país, no se haya instalado ni esté presente en la Unión y haya celebrado un acuerdo contractual con un proveedor tercero de servicios de TIC o con un proveedor tercero de servicios de TIC establecido en un tercer país;

(21) «riesgo de concentración de TIC»: una exposición a uno o múltiples proveedores terceros esenciales de servicios de TIC relacionados que cree un grado de dependencia con respecto a dichos proveedores tal que la indisponibilidad o un fallo u otro tipo de deficiencia de estos últimos pueda poner en peligro la capacidad de una entidad financiera y, en última instancia, del sistema financiero de la Unión en su conjunto, para desempeñar funciones esenciales o soportar otro tipo de efectos adversos, incluidas grandes pérdidas;

(22) «órgano de dirección»: un órgano de dirección tal como se define en el artículo 4, apartado 1, punto 36, de la Directiva 2014/65/UE, en el artículo 3, apartado 1, punto 7, de la Directiva 2013/36/UE, en el artículo 2, apartado 1, letra s), de la Directiva 2009/65/CE, en el artículo 2, apartado 1, punto 45, del Reglamento (UE) n.º 909/2014, en el artículo 3, apartado 1, punto 20, del Reglamento (UE) 2016/1011 del Parlamento Europeo y del Consejo[44], y en el artículo 3, apartado 1, letra u), del Reglamento (UE) 20xx/xx del Parlamento Europeo y del Consejo[45] [MICA], o las personas equivalentes que dirijan efectivamente la entidad o desempeñen funciones clave de conformidad con la legislación nacional o de la Unión pertinente;

(23) «entidad de crédito»: una entidad de crédito tal como se define en el artículo 4, apartado 1, punto 1, del Reglamento (UE) n.º 575/2013 del Parlamento Europeo y del Consejo[46];

(24) «empresa de servicios de inversión»: una empresa de servicios de inversión tal como se define en el artículo 4, apartado 1, punto 1, de la Directiva 2014/65/UE;

(25) «entidad de pago»: una entidad de pago tal como se define en el artículo 1, apartado 1, letra d), de la Directiva (UE) 2015/2366;

(26) «entidad de dinero electrónico»: una entidad de dinero electrónico tal como se define en el artículo 2, punto 1, de la Directiva 2009/110/CE del Parlamento Europeo y del Consejo[47];

(27) «entidad de contrapartida central»: una entidad de contrapartida central tal como se define en el artículo 2, punto 1, del Reglamento (UE) n.º 648/2012;

---

44 Reglamento (UE) 2016/1011 del Parlamento Europeo y del Consejo, de 8 de junio de 2016, sobre los índices utilizados como referencia en los instrumentos financieros y en los contratos financieros o para medir la rentabilidad de los fondos de inversión, y por el que se modifican las Directivas 2008/48/CE y 2014/17/UE y el Reglamento (UE) n.º 596/2014 (DO L 171 de 29.6.2016, p. 1).

45 [*Insértese título completo y referencia del DO*]

46 Reglamento (UE) n.º 575/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, sobre los requisitos prudenciales de las entidades de crédito y las empresas de inversión, y por el que se modifica el Reglamento (UE) n.º 648/2012 (DO L 176 de 27.6.2013, p. 1).

47 Directiva 2009/110/CE del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades, por la que se modifican las Directivas 2005/60/CE y 2006/48/CE y se deroga la Directiva 2000/46/CE (DO L 267 de 10.10.2009, p. 7).

(28) «registro de operaciones»: un registro de operaciones tal como se define en el artículo 2, punto 2, del Reglamento (UE) n.º 648/2012;

(29) «depositario central de valores»: un depositario central de valores tal como se define en el artículo 2, apartado 1, punto 1, del Reglamento (UE) n.º 909/2014;

(30) «centro de negociación» un centro de negociación tal como se define en el artículo 4, apartado 1, punto 24, de la Directiva 2014/65/UE;

(31) «gestor de fondos de inversión alternativos»: un gestor de fondos de inversión alternativos tal como se define en el artículo 4, apartado 1, letra b), de la Directiva 2011/61/UE;

(32) «sociedad de gestión»: una sociedad de gestión tal como se define en el artículo 2, apartado 1, letra b), de la Directiva 2009/65/CE;

(33) «proveedor de servicios de suministro de datos»: un proveedor de servicios de suministro de datos tal como se define en el artículo 4, apartado 1, punto 63, de la Directiva 2014/65/UE;

(34) «empresa de seguros»: una empresa de seguros tal como se define en el artículo 13, punto 1, de la Directiva 2009/138/CE;

(35) «empresa de reaseguros»: una empresa de reaseguros tal como se define en el artículo 13, punto 4, de la Directiva 2009/138/CE;

(36) «intermediario de seguros»: un intermediario de seguros tal como se define en el artículo 2, punto 3, de la Directiva (UE) 2016/97;

(37) «intermediario de seguros complementarios»: un intermediario de seguros complementarios tal como se define en el artículo 2, punto 4, de la Directiva (UE) 2016/97;

(38) «intermediario de reaseguros»: un intermediario de reaseguros tal como se define en el artículo 2, punto 5, de la Directiva (UE) 2016/97;

(39) «fondo de pensiones de empleo»: un fondo de pensiones de empleo tal como se define en el artículo 6, punto 1, de la Directiva 2016/2341;

(40) «agencia de calificación crediticia »: una agencia de calificación crediticia tal como se define en el artículo 3, apartado 1, letra a), del Reglamento (CE) n.º 1060/2009;

(41) «auditor legal»: un auditor legal tal como se define en el artículo 2, punto 2, de la Directiva 2006/43/CE;

(42) «sociedad de auditoría»: una sociedad de auditoría tal como se define en el artículo 2, punto 3, de la Directiva 2006/43/CE;

(43) «proveedor de servicios de criptoactivos»: un proveedor de servicios de criptoactivos tal como se define en el artículo 3, apartado 1, letra n), del Reglamento (UE) 202x/xx [*OP: insértese la referencia al Reglamento MICA*];

(44) «emisor de criptoactivos»: un emisor de criptoactivos tal como se define en el artículo 3, apartado 1, letra h), del [*DO: insértese la referencia al Reglamento MICA*];

(45) «emisor de fichas referenciadas a activos»: un emisor de fichas referenciadas a activos tal como se define en el artículo 3, apartado 1, letra i), del [*DO: insértese la referencia al Reglamento MICA*];

(46) «emisor de fichas significativas referenciadas a activos»: un emisor de fichas de pago significativas referenciadas a activos tal como se define en el artículo 3, apartado 1, letra j), del [*DO: insértese la referencia al Reglamento MICA*];

(47) «administrador de índices de referencia cruciales»: un administrador de índices de referencia cruciales tal como se define en el artículo x, punto x, del Reglamento xx/202x [*DO: insértese la referencia al Reglamento sobre los índices de referencia*];

(48) «proveedor de servicios de financiación participativa»: un proveedor de servicios de financiación participativa tal como se define en el artículo x, punto x, del Reglamento (UE) 202x/ xx [*OP: insértese la referencia al Reglamento relativo a la financiación participativa*];

(49) «registro de titulizaciones»: un registro de titulizaciones tal como se define en el artículo 2, punto 23, del Reglamento (UE) 2017/2402;

(50) «microempresa»: una microempresa tal como se define en el artículo 2, apartado 3, del anexo de la Recomendación 2003/361/CE.

CAPÍTULO II

GESTIÓN DE RIESGOS DE TIC

SECCIÓN I

Artículo 4

Gobernanza y organización

1. Las entidades financieras dispondrán de marcos internos de gobernanza y control que garanticen una gestión eficaz y prudente de todos los riesgos de TIC.

2. El órgano de dirección de la entidad financiera definirá, aprobará, supervisará y será responsable de la aplicación de todas las disposiciones relacionadas con el marco de gestión del riesgo de TIC a que se refiere el artículo 5, apartado 1.

   A efectos del párrafo primero, el órgano de dirección:

   (a) asumirá la responsabilidad final de gestionar los riesgos de TIC de la entidad financiera;

   (b) definirá claramente los cometidos y responsabilidades de todas las funciones relacionadas con las TIC;

   (c) determinará el nivel adecuado de tolerancia al riesgo de TIC de la entidad financiera a que se refiere el artículo 5, apartado 9, letra b);

   (d) aprobará, supervisará y revisará periódicamente la aplicación de la política de continuidad de las actividades de TIC de la entidad financiera y el plan de recuperación en caso de catástrofe relacionada con las TIC a que se refieren, respectivamente, los apartados 1 y 3 del artículo 10;

   (e) aprobará y revisará periódicamente los planes de auditoría de TIC, las auditorías de TIC y sus modificaciones significativas;

(f) asignará y revisará periódicamente el presupuesto adecuado para satisfacer las necesidades de resiliencia operativa digital de la entidad financiera con respecto a todos los tipos de recursos, incluida la formación sobre los riesgos y las competencias en materia de TIC para todo el personal pertinente;

(g) aprobará y revisará periódicamente la política de la entidad financiera sobre los acuerdos relativos al uso de servicios de TIC prestados por proveedores terceros de servicios de TIC;

(h) será debidamente informado de los acuerdos celebrados con proveedores terceros de servicios de TIC sobre el uso de servicios de TIC, de cualquier cambio sustancial pertinente previsto en relación con los proveedores terceros de servicios de TIC, y del impacto potencial de tales cambios en las funciones esenciales o importantes sujetas a dichos acuerdos, y recibirá a tal fin un resumen del análisis de riesgos para evaluar el impacto de dichos cambios;

(i) será debidamente informado sobre los incidentes relacionados con las TIC y su impacto, así como sobre las medidas de respuesta, recuperación y corrección.

3. Las entidades financieras que no sean microempresas establecerán una función de seguimiento de los acuerdos celebrados con proveedores terceros de servicios de TIC sobre el uso de servicios de TIC, o designarán a un miembro de la alta dirección como responsable de supervisar la exposición al riesgo correspondiente y la documentación pertinente.

4. Los miembros del órgano de dirección seguirán periódicamente una formación específica para adquirir y mantener al día conocimientos y competencias suficientes para comprender y evaluar los riesgos de TIC y su impacto en las operaciones de la entidad financiera.

SECCIÓN II

Artículo 5

Marco de gestión del riesgo de TIC

1. Las entidades financieras contarán con un marco de gestión del riesgo de TIC sólido, completo y bien documentado que les permita hacer frente al riesgo de TIC de forma rápida, eficiente y exhaustiva y garantizar un alto nivel de resiliencia operativa digital que se ajuste a sus necesidades, tamaño y complejidad.

2. El marco de gestión del riesgo de TIC a que se refiere el apartado 1 incluirá las estrategias, las políticas, los procedimientos, y los protocolos y herramientas de TIC que sean necesarios para proteger debida y eficazmente todas las infraestructuras y componentes físicos pertinentes, incluidos los equipos informáticos, los servidores, así como todos los locales, centros de datos y zonas sensibles designadas pertinentes, a fin de garantizar que todos esos elementos físicos estén adecuadamente protegidos de los riesgos, incluidos los daños y el acceso o uso no autorizados.

3. Las entidades financieras minimizarán el impacto del riesgo de TIC mediante el despliegue de estrategias, políticas, procedimientos, protocolos y herramientas adecuados, tal como se determine en el marco de gestión del riesgo de TIC. Proporcionarán información completa y actualizada sobre los riesgos de TIC cuando así lo exijan las autoridades competentes.

4. Como parte del marco de gestión del riesgo de TIC a que se refiere el apartado 1, las entidades financieras que no sean microempresas implementarán un sistema de gestión de la seguridad de la información basado en estándares internacionales reconocidos y conforme a las directrices de supervisión, y lo revisarán periódicamente.

5. Las entidades financieras que no sean microempresas garantizarán una separación adecuada de las funciones de gestión de TIC, las funciones de control y las funciones de auditoría interna, con arreglo a las tres líneas del modelo de defensa o a un modelo interno de gestión y control de riesgos.

6. El marco de gestión del riesgo de TIC a que se refiere el apartado 1 se documentará y revisará al menos una vez al año, así como cuando se produzcan incidentes graves relacionados con las TIC, y siguiendo las instrucciones o conclusiones de supervisión derivadas de los procesos pertinentes de prueba o auditoría de la resiliencia operativa digital. Se mejorará continuamente sobre la base de las enseñanzas derivadas de la aplicación y el seguimiento.

7. El marco de gestión del riesgo de TIC a que se refiere el apartado 1 será auditado periódicamente por auditores de TIC que posean conocimientos, competencias y experiencia suficientes en materia de riesgo de TIC. La frecuencia y el enfoque de las auditorías de TIC serán proporcionados a los riesgos de TIC de la entidad financiera.

8. Se establecerá un proceso formal de seguimiento, incluidas normas para la oportuna verificación y corrección de los resultados esenciales de la auditoría de TIC, considerando las conclusiones de la auditoría y teniendo debidamente en cuenta la naturaleza, escala y complejidad de los servicios y actividades de las entidades financieras.

9. El marco de gestión del riesgo de TIC a que se refiere el apartado 1 incluirá una estrategia de resiliencia digital que establezca cómo se aplica el marco. A tal efecto, incluirá los métodos para hacer frente al riesgo de TIC y alcanzar los objetivos específicos de TIC, para lo cual:

   (a) explicará cómo el marco de gestión del riesgo de TIC apoya la estrategia y los objetivos empresariales de la entidad financiera;

   (b) establecerá el nivel de tolerancia al riesgo de TIC, de acuerdo con la propensión al riesgo de la entidad financiera, y analizará la tolerancia al impacto de las perturbaciones de las TIC;

   (c) establecerá objetivos claros en materia de seguridad de la información;

   (d) explicará la arquitectura de referencia de TIC y cualquier cambio necesario para alcanzar objetivos empresariales específicos;

   (e) esbozará los diferentes mecanismos establecidos para detectar, prevenir y protegerse de los impactos de incidentes relacionados con las TIC;

   (f) hará constar el número de incidentes graves relacionados con las TIC notificados y la eficacia de las medidas preventivas;

   (g) definirá una estrategia holística de múltiples proveedores de TIC a nivel de entidad que muestre las dependencias clave de los proveedores terceros de servicios de TIC y explique los motivos subyacentes a la contratación de una combinación de proveedores terceros de servicios;

   (h) implementará pruebas de resiliencia operativa digital;

(i) esbozará una estrategia de comunicación en caso de incidentes relacionados con las TIC.

10. Previa aprobación de las autoridades competentes, las entidades financieras podrán delegar las tareas de verificación del cumplimiento de los requisitos de gestión del riesgo de TIC en empresas externas o de su mismo grupo.

Artículo 6

Sistemas, protocolos y herramientas de TIC

1. Las entidades financieras utilizarán y mantendrán actualizados sistemas, protocolos y herramientas de TIC que cumplan las siguientes condiciones:

(a) que los sistemas y herramientas sean adecuados a la naturaleza, variedad, complejidad y magnitud de las operaciones que sustentan la realización de sus actividades;

(b) que sean fiables;

(c) que tengan capacidad suficiente para tratar con exactitud los datos necesarios para realizar las actividades y prestar los servicios a tiempo, y para hacer frente a los picos de órdenes, mensajes o volúmenes de operaciones, según sea necesario, incluso en caso de introducción de nuevas tecnologías;

(d) que sean tecnológicamente resilientes para hacer frente adecuadamente a las necesidades adicionales de tratamiento de la información que surjan en condiciones de tensión del mercado u otras situaciones adversas.

2. Cuando las entidades financieras apliquen estándares técnicos reconocidos internacionalmente y prácticas punteras del sector en materia de seguridad de la información y controles internos de las TIC, lo harán en consonancia con cualquier recomendación de supervisión pertinente sobre su incorporación.

Artículo 7

Identificación

1. Como parte del marco de gestión del riesgo de TIC a que se refiere el artículo 5, apartado 1, las entidades financieras identificarán, clasificarán y documentarán adecuadamente todas las funciones empresariales relacionadas con las TIC, los activos de información que respalden dichas funciones, las configuraciones de los sistemas de TIC y las interconexiones con sistemas de TIC internos y externos. Las entidades financieras revisarán en caso necesario, y al menos una vez al año, la idoneidad de la clasificación de los activos de información y de cualquier documentación pertinente.

2. Las entidades financieras identificarán de forma continua todas las fuentes de riesgo de TIC, en particular la exposición al riesgo frente a otras entidades financieras, y evaluarán las ciberamenazas y vulnerabilidades de TIC pertinentes para sus funciones empresariales relacionadas con las TIC y sus activos de información. Las entidades financieras revisarán periódicamente, y al menos una vez al año, los escenarios de riesgo que les afecten.

3. Las entidades financieras que no sean microempresas llevarán a cabo una evaluación del riesgo cada vez que se produzca un cambio importante en la infraestructura de las

redes y los sistemas de información, o en los procesos o procedimientos, que afecte a sus funciones, procesos de apoyo o activos de información.

4. Las entidades financieras identificarán todas las cuentas de los sistemas de TIC, incluidas las que se encuentren en emplazamientos remotos, los recursos de red y el equipo de hardware, y cartografiarán los equipos físicos considerados críticos. Deberán cartografiar la configuración de los activos de TIC y los vínculos e interdependencias entre los distintos activos de TIC.

5. Las entidades financieras identificarán y documentarán todos los procesos que dependan de proveedores terceros de servicios de TIC, e identificarán las interconexiones con proveedores terceros de servicios de TIC.

6. A efectos de los apartados 1, 4 y 5, las entidades financieras mantendrán y actualizarán periódicamente los inventarios pertinentes.

7. Las entidades financieras que no sean microempresas llevarán a cabo periódicamente, y al menos una vez al año, una evaluación específica del riesgo de TIC en todos los sistemas de TIC heredados, especialmente antes y después de conectar tecnologías, aplicaciones o sistemas antiguos y nuevos.

Artículo 8

Protección y prevención

1. Con el fin de proteger adecuadamente los sistemas de TIC y con vistas a organizar medidas de respuesta, las entidades financieras controlarán continuamente el funcionamiento de los sistemas y herramientas de TIC y minimizarán el impacto de tales riesgos mediante el despliegue de herramientas, políticas y procedimientos de seguridad de TIC adecuados.

2. Las entidades financieras diseñarán, adquirirán y aplicarán estrategias, políticas, procedimientos, protocolos y herramientas de seguridad de las TIC que tengan por objeto, en particular, garantizar la resiliencia, la continuidad y la disponibilidad de los sistemas de TIC, así como mantener elevados niveles de seguridad, confidencialidad e integridad de los datos, con independencia de que estén en reposo, en uso o en tránsito.

3. Para alcanzar los objetivos mencionados en el apartado 2, las entidades financieras utilizarán tecnologías y procesos de TIC de última generación que:

   (a) garanticen la seguridad de los medios de transmisión de la información;

   (b) minimicen el riesgo de corrupción o pérdida de datos, acceso no autorizado y defectos técnicos que puedan obstaculizar la actividad empresarial;

   (c) eviten fugas de información;

   (d) garanticen que los datos estén protegidos de riesgos debidos a una mala administración o relacionados con el tratamiento, incluido un mantenimiento inadecuado de los registros.

4. Como parte del marco de gestión del riesgo de TIC a que se refiere el artículo 5, apartado 1, las entidades financieras deberán:

   (a) elaborar y documentar una política de seguridad de la información que defina normas para proteger la confidencialidad, integridad y disponibilidad de los

recursos de TIC, datos y activos de información, tanto de los suyos propios como de los de sus clientes;

(b) seguir un enfoque basado en el riesgo, establecer una gestión sólida de la red y de la infraestructura utilizando técnicas, métodos y protocolos adecuados, incluida la aplicación de mecanismos automatizados para aislar los activos de información afectados en caso de ciberataques;

(c) aplicar políticas que limiten el acceso físico y virtual a los recursos y datos del sistema de TIC a lo estrictamente necesario para las funciones y actividades legítimas y aprobadas, y establecer a tal efecto un conjunto de políticas, procedimientos y controles que se centren en los privilegios de acceso y una buena administración de los mismos;

(d) aplicar políticas y protocolos para mecanismos de autenticación fuerte, basados en estándares pertinentes y sistemas de control específicos para evitar el acceso a las claves criptográficas mediante las que se cifran los datos, sobre la base de los resultados de los procesos aprobados de clasificación de datos y evaluación de riesgos;

(e) aplicar políticas, procedimientos y controles para la gestión de los cambios en las TIC, incluidos los cambios en el software, el hardware, los componentes de firmware, así como los cambios en los sistemas o la seguridad, que se basen en un enfoque de evaluación de riesgos y formen parte integrante del proceso general de gestión de cambios de la entidad financiera, con el fin de garantizar que todos los cambios en los sistemas de TIC se registren, prueben, evalúen, aprueben, implementen y verifiquen de forma controlada;

(f) contar con políticas adecuadas y exhaustivas para los parches y actualizaciones.

A efectos de la letra b), las entidades financieras diseñarán la infraestructura de conexión a la red de manera que permita su desconexión instantánea y garantizarán su compartimentación y segmentación, con el fin de minimizar y prevenir el contagio, especialmente en los procesos financieros interconectados.

A efectos de la letra e), el proceso de gestión de cambios en las TIC será aprobado por la jerarquía directiva adecuada y dispondrá de protocolos específicos habilitados para los cambios de emergencia.

Artículo 9

Detección

1. Las entidades financieras dispondrán de mecanismos para detectar rápidamente las actividades anómalas, de conformidad con el artículo 15, incluidos los problemas de rendimiento de la red de TIC y los incidentes relacionados con las TIC, y para identificar todos los posibles puntos concretos de fallo significativos.

   Todos los mecanismos de detección mencionados en el párrafo primero se someterán a pruebas periódicas de conformidad con el artículo 22.

2. Los mecanismos de detección a que se refiere el apartado 1 permitirán múltiples niveles de control, definirán criterios y umbrales de alerta para activar los procesos de detección de incidentes relacionados con las TIC y de respuesta a incidentes

relacionados con las TIC, y establecerán mecanismos automáticos de alerta para el personal responsable de la respuesta a incidentes relacionados con las TIC.

3. Las entidades financieras dedicarán recursos y capacidades suficientes, teniendo debidamente en cuenta su tamaño y su perfil empresarial y de riesgo, al seguimiento de la actividad de los usuarios y la aparición de anomalías en las TIC y de incidentes relacionados con las TIC, en particular de ciberataques.

4. Las entidades financieras a que se refiere el artículo 2, apartado 1, punto 1, establecerán además sistemas que permitan controlar de manera efectiva la exhaustividad de los informes de operaciones, detectar omisiones y errores manifiestos y solicitar la retransmisión de los informes erróneos.

Artículo 10

Respuesta y recuperación

1. Como parte del marco de gestión del riesgo de TIC a que se refiere el artículo 5, apartado 1, y sobre la base de los requisitos de identificación establecidos en el artículo 7, las entidades financieras establecerán una política de continuidad de las actividades de TIC específica y exhaustiva, que formará parte integrante de la política de continuidad de la actividad operativa de la entidad financiera.

2. Las entidades financieras aplicarán la política de continuidad de las actividades de TIC a que se refiere el apartado 1 mediante disposiciones, planes, procedimientos y mecanismos específicos, adecuados y documentados destinados a:

   (a) registrar todos los incidentes relacionados con las TIC;

   (b) garantizar la continuidad de las funciones esenciales de la entidad financiera;

   (c) responder rápida, adecuada y eficazmente a todos los incidentes relacionados con las TIC, en particular, pero no exclusivamente, los ciberataques, y resolverlos, de manera que se limiten los daños y se dé prioridad a la reanudación de las actividades y a las acciones de recuperación;

   (d) activar sin demora planes específicos que permitan recurrir a medidas de contención, procesos y tecnologías adaptados a cada tipo de incidente relacionado con las TIC y que eviten nuevos daños, así como a procedimientos de respuesta y recuperación adaptados establecidos de conformidad con el artículo 11;

   (e) estimar con carácter preliminar las repercusiones, daños y pérdidas;

   (f) definir acciones de comunicación y gestión de crisis que garanticen la transmisión de información actualizada a todo el personal interno y las partes interesadas externas pertinentes de conformidad con el artículo 13, y su notificación a las autoridades competentes de conformidad con el artículo 17.

3. Como parte del marco de gestión del riesgo de TIC a que se refiere el artículo 5, apartado 1, las entidades financieras aplicarán un plan conexo de recuperación en caso de catástrofe relacionada con las TIC que, en el caso de entidades financieras que no sean microempresas, estará sujeto a auditorías independientes.

4. Las entidades financieras establecerán, mantendrán y probarán periódicamente planes adecuados de continuidad de las actividades de TIC, en particular en lo que se refiere a las funciones esenciales o importantes externalizadas o contratadas mediante acuerdos con proveedores terceros de servicios de TIC.

5. Como parte de su gestión global del riesgo de TIC, las entidades financieras:

(a) pondrán a prueba la política de continuidad de las actividades de TIC y el plan de recuperación en caso de catástrofe relacionada con las TIC al menos una vez al año y después de cambios sustanciales en los sistemas de TIC;

(b) pondrán a prueba los planes de comunicación en caso de crisis establecidos de conformidad con el artículo 13.

A efectos de la letra a), las entidades financieras que no sean microempresas incluirán en los planes de pruebas escenarios de ciberataques y de conmutación entre la infraestructura primaria de TIC y la capacidad redundante, las copias de seguridad y las instalaciones redundantes necesarias para cumplir las obligaciones establecidas en el artículo 11.

Las entidades financieras revisarán periódicamente su política de continuidad de las actividades de TIC y su plan de recuperación en caso de catástrofe relacionada con las TIC teniendo en cuenta los resultados de las pruebas realizadas de conformidad con el párrafo primero y las recomendaciones derivadas de los controles de auditoría o las revisiones supervisoras.

6. Las entidades financieras que no sean microempresas dispondrán de una función de gestión de crisis que, en caso de activación de su política de continuidad de las actividades de TIC o de su plan de recuperación en caso de catástrofe relacionada con las TIC, establecerá procedimientos claros para gestionar las comunicaciones de crisis internas y externas de conformidad con el artículo 13.

7. Las entidades financieras mantendrán registros de las actividades antes y durante las perturbaciones cuando se active su política de continuidad de las actividades de TIC o su plan de recuperación en caso de catástrofe relacionada con las TIC. Estos registros estarán fácilmente disponibles.

8. Las entidades financieras a que se refiere el artículo 2, apartado 1, letra f), facilitarán a las autoridades competentes copias de los resultados de las pruebas de continuidad de las actividades de TIC o de ejercicios similares realizados durante el período objeto de examen.

9. Las entidades financieras que no sean microempresas informarán a las autoridades competentes de todos los costes y pérdidas causados por perturbaciones de las TIC e incidentes relacionados con las TIC.

Artículo 11

Políticas de copia de seguridad y métodos de recuperación

1. Con el fin de garantizar la restauración de los sistemas de TIC con un tiempo mínimo de inactividad y una perturbación limitada, como parte de su marco de gestión del riesgo de TIC, las entidades financieras desarrollarán:

(a) una política de copia de seguridad que especifique el alcance de los datos objeto de la copia de seguridad y la frecuencia mínima de esta, en función del carácter esencial de la información o de la sensibilidad de los datos;

(b) métodos de recuperación.

2. Los sistemas de copia de seguridad comenzarán el tratamiento sin demoras indebidas, a menos que dicho inicio ponga en peligro la seguridad de las redes y los sistemas de información, o la integridad o confidencialidad de los datos.

3. Al restablecer los datos de seguridad mediante sus propios sistemas, las entidades financieras utilizarán sistemas de TIC que tengan un entorno operativo distinto del principal, que no esté directamente conectado con este último y que esté protegido de forma segura contra cualquier acceso no autorizado o corrupción relacionada con las TIC.

   En el caso de las entidades financieras a que se refiere el artículo 2, apartado 1, letra g), los planes de recuperación deberán permitir la recuperación de todas las transacciones en el momento de la perturbación, para que la entidad de contrapartida central pueda seguir operando con certeza y finalizar la liquidación en la fecha programada.

4. Las entidades financieras mantendrán capacidades de TIC redundantes equipadas con recursos, medios y funcionalidades suficientes y adecuados para satisfacer las necesidades empresariales.

5. Las entidades financieras a que se refiere el artículo 2, apartado 1, letra f), mantendrán o garantizarán que sus proveedores terceros de TIC mantengan al menos un centro secundario de procesamiento dotado de recursos, capacidades, funcionalidades y personal suficientes y adecuados para satisfacer las necesidades de las empresas.

   El centro secundario de procesamiento deberá:

   (a) estar situado a una distancia geográfica del centro primario de procesamiento para garantizar que presente un perfil de riesgo distinto y evitar que se vea afectado por el suceso que haya afectado al centro primario;

   (b) ser capaz de garantizar la continuidad de los servicios esenciales del mismo modo que el centro primario, o de prestar el nivel de servicios necesario para garantizar que la entidad financiera realice sus operaciones esenciales dentro de los objetivos de recuperación;

   (c) ser inmediatamente accesible por el personal de la entidad financiera para garantizar la continuidad de los servicios esenciales en caso de que el centro de tratamiento primario no esté disponible.

6. Al determinar los objetivos de tiempo y punto de recuperación para cada función, las entidades financieras tendrán en cuenta el posible impacto global en la eficiencia del mercado. Estos objetivos garantizarán que, en situaciones extremas, se alcancen los niveles de servicio acordados.

7. Al recuperarse de un incidente relacionado con las TIC, las entidades financieras realizarán múltiples comprobaciones, incluidas conciliaciones, a fin de garantizar que el nivel de integridad de los datos sea el máximo. Estas comprobaciones también se llevarán a cabo cuando se reconstruyan datos de partes interesadas externas, a fin de garantizar que todos los datos sean coherentes entre los sistemas.

Artículo 12

Aprendizaje y evolución

1. Las entidades financieras dispondrán de capacidades y de personal, adaptados a su tamaño y su perfil empresarial y de riesgo, para recopilar información sobre vulnerabilidades, ciberamenazas e incidentes relacionados con las TIC, en particular

ciberataques, y para analizar sus posibles repercusiones en su resiliencia operativa digital.

2. Las entidades financieras pondrán en marcha revisiones post-incidentes relacionados con las TIC después de perturbaciones significativas debidas a las TIC de sus actividades principales, analizando sus causas e identificando las mejoras necesarias en las operaciones de TIC o en la política de continuidad de las actividades de TIC a que se refiere el artículo 10.

   Cuando realicen cambios, las entidades financieras que no sean microempresas los comunicarán a las autoridades competentes.

   Las revisiones post-incidentes relacionados con las TIC a que se refiere el párrafo primero determinarán si se han seguido los procedimientos establecidos y si las medidas adoptadas han sido eficaces, en particular en relación con:

   (a) la rapidez a la hora de responder a las alertas de seguridad y determinar el impacto de los incidentes relacionados con las TIC y su gravedad;

   (b) la calidad y rapidez en la realización de los análisis forenses;

   (c) la eficacia de la activación de los niveles sucesivos de intervención en caso de incidente dentro de la entidad financiera;

   (d) la eficacia de la comunicación interna y externa.

3. Las enseñanzas derivadas de las pruebas de resiliencia operativa digital llevadas a cabo de conformidad con los artículos 23 y 24 y de los incidentes reales relacionados con las TIC, en particular los ciberataques, junto con los problemas que se hayan planteado al activar los planes de continuidad de las actividades o de recuperación, además de la información pertinente intercambiada con las contrapartes y evaluada durante las revisiones supervisoras, se incorporarán debidamente de forma continua al proceso de evaluación del riesgo de TIC. Estas constataciones se traducirán en revisiones adecuadas de los componentes pertinentes del marco de gestión del riesgo de TIC a que se refiere el artículo 5, apartado 1.

4. Las entidades financieras controlarán la eficacia de la aplicación de su estrategia de resiliencia digital establecida en el artículo 5, apartado 9. Cartografiarán la evolución de los riesgos de TIC a lo largo del tiempo, analizarán la frecuencia, los tipos, la magnitud y la evolución de los incidentes relacionados con las TIC, en particular los ciberataques y sus patrones, con el fin de comprender el nivel de exposición al riesgo de TIC y mejorar la madurez y preparación cibernéticas de la entidad financiera.

5. El personal directivo responsable de las TIC informará al menos una vez al año al órgano de dirección de las constataciones a que se refiere el apartado 3 y formulará recomendaciones.

6. Las entidades financieras desarrollarán programas de sensibilización en materia de seguridad de las TIC y acciones formativas sobre resiliencia operativa digital, que constituirán módulos obligatorios en sus programas de formación del personal. Estos módulos serán aplicables a todos los empleados y al personal de alta dirección.

   Las entidades financieras supervisarán continuamente los avances tecnológicos pertinentes, también con vistas a comprender las posibles repercusiones del despliegue de esas nuevas tecnologías en los requisitos de seguridad de las TIC y la resiliencia operativa digital. Se mantendrán al corriente de los últimos procesos de

gestión del riesgo de TIC, contrarrestando eficazmente las formas actuales o nuevas de ciberataques.

Artículo 13
Comunicación

1. Como parte del marco de gestión del riesgo de TIC a que se refiere el artículo 5, apartado 1, las entidades financieras dispondrán de planes de comunicación que permitan la divulgación responsable de incidentes relacionados con las TIC o vulnerabilidades importantes a clientes y contrapartes, así como al público, según proceda.
2. Como parte del marco de gestión del riesgo de TIC a que se refiere el artículo 5, apartado 1, las entidades financieras aplicarán políticas de comunicación destinadas al personal y las partes interesadas externas. Las políticas de comunicación destinadas al personal tendrán en cuenta la necesidad de diferenciar entre el personal que participa en la gestión del riesgo de TIC, en particular en la respuesta y la recuperación, y el personal que debe ser informado.
3. Al menos una persona de la entidad se encargará de aplicar la estrategia de comunicación sobre incidentes relacionados con las TIC y desempeñará a tal efecto la función de portavoz ante el público y los medios de comunicación.

Artículo 14
Mayor armonización de las herramientas, métodos, procesos y políticas de gestión del riesgo de TIC

La Autoridad Bancaria Europea (ABE), la Autoridad Europea de Valores y Mercados (AEVM) y la Autoridad Europea de Seguros y Pensiones de Jubilación (AESPJ), en consulta con la Agencia de la Unión Europea para la Ciberseguridad (ENISA), elaborarán proyectos de normas técnicas de regulación con los siguientes fines:

(a) especificar otros elementos que deban incluirse en las políticas, procedimientos, protocolos y herramientas de seguridad de las TIC a que se refiere el artículo 8, apartado 2, con vistas a garantizar la seguridad de las redes, activar salvaguardias adecuadas contra las intrusiones y el uso indebido de los datos, preservar la autenticidad e integridad de los datos, incluidas las técnicas criptográficas, y garantizar una transmisión exacta y rápida de los datos sin perturbaciones importantes;

(b) prescribir cómo deberán las políticas, procedimientos y herramientas de seguridad de las TIC a que se refiere el artículo 8, apartado 2, incorporar controles de seguridad a los sistemas desde el principio (seguridad desde el diseño), permitir ajustarse a la naturaleza cambiante de las amenazas y prever el uso de tecnología de defensa en profundidad;

(c) especificar más detalladamente las técnicas, métodos y protocolos apropiados a que se refiere el artículo 8, apartado 4, letra b);

(d) desarrollar nuevos componentes de los controles de los derechos de gestión de acceso a que se refiere el artículo 8, apartado 4, letra c), y la correspondiente política de recursos humanos, especificando los derechos de acceso, los procedimientos de concesión y revocación de derechos, el seguimiento de comportamientos anómalos en relación con los riesgos de TIC a través de

indicadores adecuados, en particular para los patrones de uso de la red, las horas, la actividad informática y los dispositivos desconocidos;

(e) desarrollar más detalladamente los elementos especificados en el artículo 9, apartado 1, que permitan la rápida detección de actividades anómalas y los criterios mencionados en el artículo 9, apartado 2, que activen los procesos de detección de incidentes relacionados con las TIC y de respuesta a los mismos;

(f) especificar más detalladamente los componentes de la política de continuidad de las actividades de TIC a que se refiere el artículo 10, apartado 1;

(g) especificar más detalladamente las pruebas de los planes de continuidad de las actividades de TIC a que se refiere el artículo 10, apartado 5, a fin de garantizar que tengan debidamente en cuenta los escenarios en los que la calidad de la ejecución de una función esencial o importante se deteriore hasta un nivel inaceptable o falle, así como el impacto potencial de la insolvencia u otros fallos de cualquier proveedor tercero de servicios de TIC pertinente y, cuando proceda, los riesgos políticos en los países de los proveedores de que se trate;

(h) especificar más detalladamente los componentes del plan de recuperación en caso de catástrofe relacionada con las TIC a que se refiere el artículo 10, apartado 3.

La ABE, la AEVM y la AESPJ presentarán a la Comisión el proyecto de normas técnicas de regulación a más tardar el xxx [*DO: insértese la fecha correspondiente a 1 año después de la fecha de entrada en vigor*].

Se delegan en la Comisión los poderes para adoptar las normas técnicas de regulación a que se refiere el párrafo primero de conformidad con los artículos 10 a 14 del Reglamento (UE) n.º 1093/2010, el Reglamento (UE) n.º 1094/2010 y el Reglamento (UE) n.º 1095/2010.

CAPÍTULO III

INCIDENTES RELACIONADOS CON LAS TIC

GESTIÓN, CLASIFICACIÓN e INFORMACIÓN

Artículo 15

Proceso de gestión de incidentes relacionados con las TIC

4. Las entidades financieras establecerán e implementarán un proceso de gestión de incidentes relacionados con las TIC para detectar, gestionar y notificar dichos incidentes y dispondrán de indicadores de alerta temprana.

5. Las entidades financieras establecerán los procesos adecuados para que los incidentes relacionados con las TIC sean objeto de un seguimiento, un tratamiento y una respuesta coherentes e integrados, a fin de asegurarse de que se determinen y erradiquen las causas subyacentes para evitar que se produzcan.

6. El proceso de gestión de incidentes relacionados con las TIC mencionado en el apartado 1:

(i) establecerá procedimientos para identificar, rastrear, registrar, categorizar y clasificar los incidentes relacionados con las TIC en función de su prioridad y

de la gravedad y el carácter esencial de los servicios afectados, conforme a los criterios a que se hace referencia en el artículo 16, apartado 1;

(j) asignará funciones y responsabilidades que deberán activarse para los diferentes tipos y escenarios de incidentes relacionados con las TIC;

(k) expondrá planes para la comunicación con el personal, las partes interesadas externas y los medios de comunicación de conformidad con el artículo 13, para la notificación a los clientes, procedimientos internos de traslado a la instancia jerárquica superior, que abarquen también las reclamaciones de los clientes relacionadas con las TIC, así como para el suministro de información a las entidades financieras que actúen como contraparte, cuando proceda;

(l) garantizará que los incidentes graves relacionados con las TIC se pongan en conocimiento de los altos directivos pertinentes y que se informe de ellos al órgano de dirección, explicando sus repercusiones, las medidas adoptadas como respuesta y los controles adicionales que se prevé implantar como resultado de los incidentes relacionados con las TIC;

(m) establecerá procedimientos de respuesta a los incidentes relacionados con las TIC para mitigar sus repercusiones y garantizar que los servicios sean nuevamente operativos y seguros de manera oportuna.

Artículo 16

Clasificación de los incidentes relacionados con las TIC

7. Las entidades financieras clasificarán los incidentes relacionados con las TIC y determinarán su repercusión con arreglo a los siguientes criterios:

(n) número de usuarios o de contrapartes financieras afectados por la perturbación causada por el incidente relacionado con las TIC, y si dicho incidente ha repercutido en la reputación;

(o) duración del incidente relacionado con las TIC, incluida la duración de la interrupción del servicio;

(p) extensión geográfica de las zonas afectadas por el incidente relacionado con las TIC, en especial si afecta a más de dos Estados miembros;

(q) pérdidas de datos que el incidente relacionado con las TIC acarree, en términos de pérdida de integridad, pérdida de confidencialidad o pérdida de disponibilidad;

(r) gravedad de la repercusión del incidente relacionado con las TIC en los sistemas de TIC de la entidad financiera;

(s) carácter esencial de los servicios afectados, incluidas las transacciones y operaciones de la entidad financiera;

(t) repercusión económica del incidente relacionado con las TIC tanto en términos absolutos como relativos.

8. Las AES, a través del Comité Mixto de las AES (en lo sucesivo, «el Comité Mixto») y previa consulta al Banco Central Europeo (BCE) y la ENISA, elaborarán proyectos de normas técnicas de regulación comunes en las que se especificará más detalladamente lo siguiente:

(u) los criterios expuestos en el apartado 1, y en concreto los umbrales de importancia relativa para determinar los incidentes graves relacionados con las TIC que están sujetos al requisito de información establecido en el artículo 17, apartado 1;

(v) los criterios que deberán aplicar las autoridades competentes para evaluar la significación de los incidentes graves relacionados con las TIC para otros Estados miembros, y los datos de los informes sobre los incidentes relacionados con las TIC que deberán compartirse con las demás autoridades competentes de conformidad con el artículo 17, apartados 5 y 6.

9. Cuando elaboren los proyectos de normas técnicas de regulación comunes a que se refiere el apartado 2, las AES tendrán en cuenta las normas internacionales, así como las especificaciones elaboradas y publicadas por la ENISA, incluidas, cuando proceda, las especificaciones para otros sectores económicos.

Las AES presentarán a la Comisión dichos proyectos de normas técnicas de regulación comunes a más tardar el [*OP: insértese la fecha correspondiente a 1 año después de la fecha de entrada en vigor*].

Se delegan en la Comisión los poderes para completar el presente Reglamento mediante la adopción de las normas técnicas de regulación a que se refiere el apartado 2 de conformidad con los artículos 10 a 14 del Reglamento (UE) n.º 1093/2010, del Reglamento (UE) n.º 1094/2010 y del Reglamento (UE) n.º 1095/2010.

Artículo 17

Notificación de los incidentes graves relacionados con las TIC

10. Las entidades financieras notificarán los incidentes graves relacionados con las TIC a la autoridad competente pertinente a que se refiere el artículo 41, dentro de los plazos establecidos en el apartado 3.

A los efectos del párrafo primero, tras recopilar y analizar toda la información pertinente las entidades financieras elaborarán un informe del incidente utilizando la plantilla a que se refiere el artículo 18 y lo presentarán a la autoridad competente.

El informe incluirá toda la información necesaria para que la autoridad competente pueda determinar la significatividad del incidente grave relacionado con las TIC y evaluar sus posibles efectos transfronterizos.

11. Cuando un incidente grave relacionado con las TIC haya afectado o pueda afectar a los intereses financieros de los usuarios de sus servicios y clientes, las entidades financieras informarán sin dilación indebida de dicho incidente a los usuarios de sus servicios y clientes y, lo antes posible, les comunicarán todas las medidas que se hayan adoptado para mitigar sus consecuencias adversas.

12. Las entidades financieras presentarán a la autoridad competente a que se refiere el artículo 41:

(w) una notificación inicial, sin dilación, y en todo caso antes de que finalice el día hábil, o, si el incidente grave relacionado con las TIC se ha producido menos de dos horas antes de que finalice el día hábil, a más tardar cuatro horas después del comienzo del día hábil siguiente, o, cuando los canales de transmisión de información no estén disponibles, tan pronto como lo estén;

(x) un informe intermedio, a más tardar una semana después de la notificación inicial a que se refiere la letra a), seguido cuando sea necesario de notificaciones actualizadas cada vez que se disponga de una actualización pertinente de la situación, y siempre que lo solicite expresamente la autoridad competente;

(y) un informe final, cuando haya concluido el análisis de la causa subyacente, con independencia de que se hayan aplicado ya o no medidas paliativas, y cuando se disponga de las cifras reales de incidencia para sustituir a las estimaciones, pero no más tarde de un mes desde el envío del informe inicial.

13. Las entidades financieras solo podrán delegar las obligaciones de información establecidas en el presente artículo en un proveedor tercero de servicios una vez que la autoridad competente pertinente a que se refiere el artículo 41 haya aprobado la delegación.

14. La autoridad competente, una vez que reciba el informe a que se refiere el apartado 1, facilitará sin dilación indebida los datos detallados sobre el incidente a:

(z) la ABE, la AEVM o la AESPJ, según proceda;

(aa) el BCE, según proceda, en el caso de las entidades financieras a las que se refiere el artículo 2, apartado 1, letras a), b) y c); y

(bb) el punto de contacto único designado con arreglo a lo dispuesto en el artículo 8 de la Directiva (UE) 2016/1148.

15. La ABE, la AEVM o la AESPJ y el BCE evaluarán la pertinencia del incidente grave relacionado con las TIC para otras autoridades públicas pertinentes y las informarán según corresponda lo antes posible. El BCE notificará las cuestiones pertinentes para el sistema de pagos a los miembros del Sistema Europeo de Bancos Centrales. Basándose en dicha notificación, las autoridades competentes tomarán, en su caso, las medidas necesarias para proteger la estabilidad inmediata del sistema financiero.

Artículo 18

Armonización del contenido de la información y las plantillas para presentarla

16. Las AES, a través del Comité Mixto y previa consulta a la ENISA y al BCE, elaborarán:

(cc) proyectos de normas técnicas de regulación comunes al objeto de:

(1) establecer el contenido de la información que deberá presentarse cuando se produzcan incidentes graves relacionados con las TIC;

(2) especificar las condiciones en las que las entidades financieras podrán delegar en un proveedor tercero de servicios, previa aprobación de la autoridad competente, las obligaciones de información establecidas en el presente capítulo;

(dd) proyectos de normas técnicas de ejecución comunes para establecer los formularios, las plantillas y los procedimientos normalizados que deberán utilizar las entidades financieras para informar de un incidente grave relacionado con las TIC.

Las AES presentarán a la Comisión los proyectos de normas técnicas de regulación comunes a que se refiere el apartado 1, letra a), y los proyectos de normas técnicas de ejecución comunes a que se refiere el apartado 1, letra b), a más tardar, el xx 202x [*OP: insértese la fecha correspondiente a 1 año después de la fecha de entrada en vigor*].

Se delegan en la Comisión los poderes para completar el presente Reglamento mediante la adopción de las normas técnicas de regulación comunes a que se refiere el apartado 1, letra a), de conformidad con los artículos 10 a 14 del Reglamento (UE) n.º 1093/2010, el Reglamento (UE) n.º 1095/2010 y el Reglamento (UE) n.º 1094/2010.

Se otorgan a la Comisión competencias para adoptar las normas técnicas de ejecución comunes a que se refiere el apartado 1, letra b), de conformidad con el artículo 15 del Reglamento (UE) n.º 1093/2010, el Reglamento (UE) n.º 1095/2010 y el Reglamento (UE) n.º 1094/2010.

Artículo 19

Centralización de la información sobre los incidentes graves relacionados con las TIC

17. Las AES, a través del Comité Mixto y en consulta con el BCE y la ENISA, prepararán un informe conjunto en el que se evaluará la viabilidad de centralizar más la información sobre incidentes mediante la creación de un centro único de la UE para la presentación de información sobre incidentes graves relacionados con las TIC por las entidades financieras. En el informe se estudiarán maneras de facilitar la circulación de la información sobre incidentes graves relacionados con las TIC, reducir los costes asociados y sustentar análisis temáticos con el fin de mejorar la convergencia de la supervisión.

18. El informe al que se refiere el apartado 1 incluirá al menos los siguientes elementos:

(ee) requisitos previos para la creación de ese centro de la UE;

(ff) ventajas, limitaciones y posibles riesgos;

(gg) elementos de gestión operativa;

(hh) condiciones de participación;

(ii) modalidades de acceso al centro de la UE para las entidades financieras y las autoridades nacionales competentes;

(jj) evaluación preliminar de los costes financieros que conllevaría la creación de la plataforma operativa que sustentaría el centro de la UE, incluidos los conocimientos técnicos necesarios.

19. Las AES presentarán el informe a que se refiere el apartado 1 a la Comisión, al Parlamento Europeo y al Consejo a más tardar el xx 202x [*OP: insértese la fecha correspondiente a 3 años después de la fecha de entrada en vigor*].

Artículo 20

Respuesta de las autoridades de la supervisión

20. Cuando reciba un informe como el mencionado en el artículo 17, apartado 1, la autoridad competente acusará recibo de la notificación y proporcionará con la mayor celeridad posible todos los comentarios o la orientación que sean necesarios a la

entidad financiera, en particular para estudiar medidas correctoras a nivel de la entidad o formas de minimizar las repercusiones negativas en diferentes sectores.

21. Las AES, a través del Comité Mixto, informarán anualmente, utilizando datos anonimizados y agregados, sobre las notificaciones de incidentes relacionados con las TIC recibidas de las autoridades competentes, indicando al menos el número de incidentes graves relacionados con las TIC, su naturaleza, su repercusión en las operaciones de las entidades financieras o de los clientes, los costes y las medidas correctoras tomadas.

Las AES publicarán advertencias y elaborarán estadísticas de alto nivel para apoyar las evaluaciones de las amenazas y las vulnerabilidades que afecten a las TIC.

CAPÍTULO IV

PRUEBAS DE RESILIENCIA OPERATIVA DIGITAL

Artículo 21

Requisitos generales para la realización de pruebas de resiliencia operativa digital

22. A fin de evaluar el estado de preparación ante incidentes relacionados con las TIC, o de detectar debilidades, deficiencias o carencias en la resiliencia operativa digital y de aplicar sin demora medidas correctoras, las entidades financieras establecerán, mantendrán y revisarán, teniendo debidamente en cuenta su tamaño y su perfil empresarial y de riesgo, un programa de pruebas de resiliencia operativa digital sólido y completo que forme parte del marco de gestión del riesgo de TIC a que se refiere el artículo 5.

23. El programa de pruebas de resiliencia operativa digital incluirá una serie de evaluaciones, pruebas, métodos, prácticas y herramientas que se aplicarán conforme a lo dispuesto en los artículos 22 y 23.

24. Las entidades financieras seguirán un enfoque basado en el riesgo cuando lleven a cabo el programa de pruebas de resiliencia operativa digital a que se refiere el apartado 1, teniendo en cuenta el panorama cambiante de los riesgos de TIC, cualesquiera riesgos específicos a los que la entidad financiera esté o pueda estar expuesta, el carácter esencial de los activos de información y de los servicios prestados, así como cualquier otro factor que la entidad financiera considere apropiado.

25. Las entidades financieras se asegurarán de que las pruebas sean realizadas por partes independientes, ya sean internas o externas.

26. Las entidades financieras establecerán procedimientos y políticas para ordenar por prioridades, clasificar y corregir todos los problemas detectados durante la realización de las pruebas y establecerán métodos de validación interna para asegurarse de que todas las debilidades, deficiencias o carencias sean tratadas de manera exhaustiva.

27. Las entidades financieras probarán todos los sistemas y aplicaciones de TIC esenciales al menos una vez al año.

Artículo 22

Pruebas de las herramientas y los sistemas de TIC

28. El programa de pruebas de resiliencia operativa digital a que se refiere el artículo 21 dispondrá la ejecución de un conjunto completo de pruebas adecuadas, que incluirá evaluaciones y exploraciones de vulnerabilidad, análisis del código abierto, evaluaciones de seguridad de la red, análisis de carencias, exámenes de la seguridad física, cuestionarios y soluciones de software de detección, revisiones del código fuente cuando sea posible, pruebas basadas en escenarios, pruebas de compatibilidad, pruebas de rendimiento, pruebas de extremo a extremo o pruebas de penetración.

29. Las entidades financieras a que se refiere el artículo 2, apartado 1, letras f) y g), llevarán a cabo evaluaciones de vulnerabilidad antes de implantar o reimplantar servicios nuevos o ya existentes que sustenten componentes de las funciones, aplicaciones e infraestructuras esenciales de la entidad financiera.

Artículo 23

Pruebas avanzadas de las herramientas, los sistemas y los procesos de TIC basadas en pruebas de penetración guiadas por amenazas

30. Las entidades financieras determinadas de conformidad con el apartado 4 llevarán a cabo al menos cada tres años pruebas avanzadas consistentes en pruebas de penetración guiadas por amenazas.

31. Las pruebas de penetración guiadas por amenazas abarcarán al menos las funciones y los servicios esenciales de una entidad financiera y se realizarán sobre los sistemas de producción en vivo que sustenten esas funciones. El alcance preciso de las pruebas de penetración guiadas por amenazas, basado en el examen de las funciones y los servicios esenciales, será definido por las entidades financieras y validado por las autoridades competentes.

A efectos de lo dispuesto en el párrafo primero, las entidades financieras determinarán todos los procesos, sistemas y tecnologías subyacentes que sustenten funciones y servicios esenciales, incluidos los servicios y funciones externalizados o contratados a proveedores terceros de servicios de TIC.

Cuando haya proveedores terceros de servicios de TIC incluidos en el ámbito de cobertura de las pruebas de penetración guiadas por amenazas, la entidad financiera tomará las medidas necesarias para asegurar la participación de estos proveedores.

Las entidades financieras aplicarán controles efectivos de gestión del riesgo para reducir los riesgos de cualquier posible repercusión en los datos, daño de los activos y perturbación de servicios u operaciones esenciales en la propia entidad financiera, en sus contrapartes o en el sector financiero.

Al finalizar la prueba, y una vez que se hayan aprobado los informes y los planes correctores, la entidad financiera y los testadores externos facilitarán a la autoridad competente la documentación que confirme que la prueba de penetración guiada por amenazas se ha realizado conforme a los requisitos. Las autoridades competentes validarán la documentación y expedirán un certificado.

32. Las entidades financieras contratarán de conformidad con el artículo 24 a los testadores que realizarán las pruebas de penetración guiadas por amenazas.

Las autoridades competentes determinarán las entidades financieras que deberán realizar pruebas de penetración guiadas por amenazas de manera proporcionada al tamaño, la escala, la actividad y el perfil de riesgo global de la entidad financiera, basándose en la evaluación de:

(kk) factores relacionados con la repercusión, en particular el carácter esencial de los servicios prestados y las actividades realizadas por la entidad financiera;

(ll) posibles problemas de estabilidad financiera, y en concreto el carácter sistémico de la entidad financiera a nivel nacional o de la Unión, cuando proceda;

(mm) el perfil de riesgo de TIC específico, el nivel de madurez de las TIC de la entidad financiera o las características tecnológicas presentes.

33. La ABE, la AEVM y la AESPJ, previa consulta al BCE y teniendo en cuenta los marcos pertinentes de la Unión aplicables a las pruebas de penetración basadas en inteligencia, elaborarán proyectos de normas técnicas de regulación para especificar con más detalle:

(nn) los criterios utilizados a efectos de la aplicación del apartado 6 del presente artículo;

(oo) los requisitos en relación con:

(a) el alcance de las pruebas de penetración guiadas por amenazas a que se refiere el apartado 2 del presente artículo;

(b) la metodología y el enfoque de realización de pruebas que deberán seguirse para cada fase específica del proceso de prueba;

(c) las fases de resultados, conclusión y adopción de medidas correctoras del proceso de prueba;

(pp) el tipo de cooperación entre autoridades supervisoras necesaria para llevar a cabo pruebas de penetración guiadas por amenazas en el contexto de entidades financieras que operen en más de un Estado miembro, para permitir un nivel adecuado de participación de los supervisores y una ejecución flexible que tenga en cuenta las características específicas de subsectores financieros o mercados financieros locales.

Las AES presentarán a la Comisión dichos proyectos de normas técnicas de regulación a más tardar el [*OP: insértese la fecha correspondiente a 2 meses antes de la fecha de entrada en vigor*].

Se delegan en la Comisión los poderes para completar el presente Reglamento mediante la adopción de las normas técnicas de regulación a que se refiere el párrafo segundo de conformidad con los artículos 10 a 14 del Reglamento (UE) n.º 1093/2010, el Reglamento (UE) n.º 1095/2010 y el Reglamento (UE) n.º 1094/2010.

Artículo 24

Requisitos aplicables a los testadores

34. Para la realización de pruebas de penetración guiadas por amenazas, las entidades financieras solo recurrirán a testadores que:

(qq) tengan el más alto grado de idoneidad y prestigio;

(rr) posean capacidades técnicas y organizativas y demuestren una pericia técnica específica en inteligencia sobre amenazas, pruebas de penetración o pruebas de equipo rojo;

(ss) estén acreditados por un órgano de certificación de un Estado miembro o adheridos a códigos de conducta o marcos éticos oficiales;

(tt) en el caso de los testadores externos, proporcionen una garantía independiente o un informe de auditoría que acrediten la buena gestión de los riesgos asociados con la ejecución de pruebas de penetración guiadas por amenazas, incluidas la protección adecuada de la información confidencial de la entidad financiera y medidas correctoras para contrarrestar los riesgos operativos de esta;

(uu) en el caso de los testadores externos, estén debida y completamente cubiertos por los seguros pertinentes de responsabilidad civil profesional, en particular frente a los riesgos de conducta indebida y negligencia.

35. Las entidades financieras se asegurarán de que los acuerdos celebrados con testadores externos exijan una buena gestión de los resultados de las pruebas de penetración guiadas por amenazas y de que ningún tratamiento del que sean objeto, incluido cualquier proceso de generación, redacción, almacenamiento, agregación, información, comunicación o destrucción, cree riesgos para la entidad financiera.

CAPÍTULO V

GESTIÓN DEL RIESGO DE TERCEROS RELACIONADO CON LAS TIC

SECCIÓN I

PRINCIPIOS FUNDAMENTALES DE UNA BUENA GESTIÓN DEL RIESGO DE TERCEROS RELACIONADO CON LAS TIC

Artículo 25

Principios generales

Las entidades financieras gestionarán el riesgo de terceros relacionado con las TIC como un elemento integrante del riesgo de TIC dentro de su marco de gestión del riesgo de TIC y de conformidad con los principios siguientes:

36. Las entidades financieras que tengan acuerdos contractuales en vigor para utilizar servicios de TIC en la realización de sus operaciones empresariales serán en todo momento plenamente responsables del acatamiento y el cumplimiento de todas las obligaciones que se deriven del presente Reglamento y de la legislación sobre servicios financieros aplicable.

37. Las entidades financieras gestionarán el riesgo de terceros relacionado con las TIC con arreglo al principio de proporcionalidad, teniendo en cuenta:

(vv) la magnitud, la complejidad y la importancia de las dependencias con respecto a las TIC;

(ww) los riesgos derivados de los acuerdos contractuales sobre el uso de servicios de TIC celebrados con proveedores terceros de servicios de TIC, teniendo en cuenta el carácter esencial o la importancia del servicio, el proceso o la función de que se trate, y la repercusión potencial en la continuidad y la calidad de las actividades y los servicios financieros, a nivel individual y de grupo.

38. Como parte de su marco de gestión del riesgo de TIC, las entidades financieras adoptarán una estrategia, que revisarán periódicamente, sobre el riesgo de terceros relacionado con las TIC, teniendo en cuenta la estrategia de múltiples proveedores a que se refiere el artículo 5, apartado 9, letra g). Esa estrategia incluirá una política sobre el uso de servicios de TIC prestados por proveedores terceros de servicios de TIC y se aplicará a nivel individual y, cuando proceda, en base subconsolidada y consolidada. El órgano de dirección revisará periódicamente los riesgos detectados por lo que respecta a la externalización de funciones esenciales o importantes.

39. Como parte de su marco de gestión del riesgo de TIC, las entidades financieras mantendrán y actualizarán a nivel individual, y a nivel subconsolidado y consolidado, un registro de información en relación con todos los acuerdos contractuales sobre el uso de servicios de TIC prestados por proveedores terceros.

Los acuerdos contractuales a que se refiere el párrafo primero se documentarán adecuadamente, distinguiendo entre los que comprendan funciones esenciales o importantes y los que no.

Las entidades financieras comunicarán al menos una vez al año a las autoridades competentes información sobre el número de nuevos acuerdos relativos al uso de servicios de TIC, las categorías de proveedores terceros de servicios de TIC, el tipo de acuerdos contractuales y los servicios y funciones prestados.

Las entidades financieras pondrán a disposición de la autoridad competente, previa solicitud, el registro completo de información o, cuando así se solicite, secciones específicas de este, junto con toda información que se considere necesaria para permitir la supervisión efectiva de la entidad financiera.

Las entidades financieras informarán oportunamente a la autoridad competente cuando se propongan contratar funciones esenciales o importantes y cuando una función se haya convertido en esencial o importante.

40. Antes de celebrar un acuerdo contractual sobre el uso de servicios de TIC, las entidades financieras:

(xx) evaluarán si el acuerdo contractual se refiere a una función esencial o importante;

(yy) evaluarán si se cumplen las condiciones de supervisión para la contratación;

(zz) determinarán y evaluarán todos los riesgos pertinentes en relación con el acuerdo contractual, incluida la posibilidad de que dicho acuerdo pueda contribuir a reforzar el riesgo de concentración de TIC;

(aaa) llevarán a cabo todas las comprobaciones debidas con respecto a los posibles proveedores terceros de servicios de TIC y se asegurarán, a través de los procesos de selección y evaluación, de la idoneidad de dichos proveedores;

(bbb) determinarán y evaluarán los conflictos de intereses que el acuerdo contractual pueda causar.

41. Las entidades financieras únicamente podrán celebrar acuerdos contractuales con proveedores terceros de servicios de TIC que cumplan unas normas estrictas, adecuadas y actualizadas en materia de seguridad de la información.

42. Al ejercer los derechos de acceso, inspección y auditoría sobre el proveedor tercero de servicios de TIC, las entidades financieras determinarán previamente, con arreglo a un enfoque basado en el riesgo, la frecuencia de las auditorías e inspecciones y los ámbitos que deben auditarse, según normas de auditoría comúnmente aceptadas en consonancia con las instrucciones de supervisión sobre el uso y la incorporación de dichas normas de auditoría.

En el caso de los acuerdos contractuales que impliquen un alto nivel de complejidad tecnológica, la entidad financiera verificará que los auditores, ya sean internos, grupos de auditores o auditores externos, posean las capacidades y los conocimientos adecuados para llevar a cabo eficazmente las auditorías y evaluaciones pertinentes.

43. Las entidades financieras se asegurarán de que se ponga término a los acuerdos contractuales sobre el uso de servicios de TIC al menos en los siguientes casos:

(ccc) incumplimiento por parte del proveedor tercero de servicios de TIC de las disposiciones legales o reglamentarias o de las cláusulas contractuales aplicables;

(ddd) circunstancias observadas durante el seguimiento del riesgo de terceros relacionado con las TIC que se considere que pueden alterar el desempeño de las funciones prestadas en virtud del acuerdo contractual, incluidos cambios significativos que afecten al acuerdo o a la situación del proveedor tercero de servicios de TIC;

(eee) deficiencias manifiestas del proveedor tercero de servicios de TIC en su gestión global del riesgo de TIC y, en particular, en la forma en que garantiza la seguridad e integridad de los datos confidenciales, personales o sensibles en general o de la información no personal;

(fff) cuando la autoridad competente haya dejado de poder supervisar eficazmente a la entidad financiera como resultado del acuerdo contractual de que se trate.

44. Las entidades financieras establecerán estrategias de salida para tener en cuenta los riesgos que puedan surgir en relación con el proveedor tercero de servicios de TIC, en particular un posible fallo de este último, un deterioro de la calidad de las funciones ofrecidas, cualquier perturbación de la actividad debida a una falta de prestación de servicios o a una prestación inadecuada, o un riesgo sustancial que pueda plantearse en relación con el ejercicio adecuado y continuo de la función.

Las entidades financieras se asegurarán de poder abandonar los acuerdos contractuales sin:

(ggg) perturbación de sus actividades comerciales;

(hhh) limitación del cumplimiento de los requisitos reglamentarios;

(iii) perjuicio para la continuidad y la calidad de su prestación de servicios a los clientes.

Los planes de salida serán exhaustivos, estarán documentados y, en su caso, habrán sido suficientemente probados.

Las entidades financieras identificarán soluciones alternativas y elaborarán planes de transición que les permitan recuperar las funciones contratadas y los datos pertinentes del proveedor tercero de servicios de TIC y transferirlos de forma segura e íntegra a proveedores alternativos o reincorporarlos internamente.

Las entidades financieras adoptarán las medidas de contingencia adecuadas para mantener la continuidad de sus actividades en todas las circunstancias mencionadas en el párrafo primero.

45. Las AES, a través del Comité Mixto, elaborarán proyectos de normas técnicas de ejecución a fin de establecer las plantillas normalizadas para del registro de información a que se refiere el apartado 4.

Las AES presentarán a la Comisión dichos proyectos de normas técnicas de ejecución a más tardar el [*OP: insértese la fecha correspondiente a 1 año después de la fecha de entrada en vigor*].

Se otorgan a la Comisión competencias para adoptar las normas técnicas de ejecución a que se refiere el párrafo primero de conformidad con el artículo 15 del Reglamento (UE) n.º 1093/2010, el Reglamento (UE) n.º 1095/2010 y el Reglamento (UE) n.º 1094/2010.

46. Las AES, a través del Comité Mixto, elaborarán proyectos de normas técnicas de regulación:

(jjj) para especificar el contenido detallado de la política a que se refiere el apartado 3 en relación con los acuerdos contractuales sobre el uso de servicios de TIC prestados por proveedores terceros, con referencia a las principales fases del ciclo de vida de los correspondientes acuerdos sobre el uso de servicios de TIC;

(kkk) los tipos de información que deberán figurar en el registro de información al que se refiere el apartado 4.

Las AES presentarán a la Comisión dichos proyectos de normas técnicas de regulación a más tardar el [*OP: insértese la fecha correspondiente a 1 año después de la fecha de entrada en vigor*].

Se delegan en la Comisión los poderes para completar el presente Reglamento mediante la adopción de las normas técnicas de regulación a que se refiere el párrafo segundo de conformidad con los artículos 10 a 14 del Reglamento (UE) n.º 1093/2010, el Reglamento (UE) n.º 1095/2010 y el Reglamento (UE) n.º 1094/2010.

Artículo 26

Evaluación preliminar del riesgo de concentración de TIC y posteriores acuerdos de subexternalización

47. Al llevar a cabo la determinación y evaluación del riesgo de concentración de TIC a que se refiere el artículo 25, apartado 5, letra c), las entidades financieras tendrán en cuenta si la celebración de un acuerdo contractual en relación con los servicios de TIC puede dar lugar a alguna de las siguientes circunstancias:

(lll) la celebración de un contrato con un proveedor tercero de servicios de TIC que no sea fácilmente sustituible; o

(mmm) la coexistencia de múltiples acuerdos contractuales en relación con la prestación de servicios de TIC con el mismo proveedor tercero de servicios de

TIC o con proveedores terceros de servicios de TIC estrechamente relacionados.

Las entidades financieras ponderarán los beneficios y los costes de soluciones alternativas, como el recurso a distintos proveedores terceros de servicios de TIC, considerando si las soluciones contempladas se ajustan a las necesidades y objetivos empresariales establecidos en su estrategia de resiliencia digital y de qué manera.

48. Cuando el acuerdo contractual sobre el uso de servicios de TIC incluya la posibilidad de que un proveedor tercero de servicios de TIC subcontrate a su vez una función esencial o importante a otros proveedores terceros de servicios de TIC, las entidades financieras ponderarán los beneficios y los riesgos que puedan derivarse de esa posible subcontratación, en particular cuando se trate de un subcontratista de TIC establecido en un tercer país.

Cuando se celebren acuerdos contractuales sobre el uso de servicios de TIC con un proveedor tercero de servicios de TIC establecido en un tercer país, las entidades financieras considerarán relevantes, al menos, los siguientes factores:

(nnn) el respeto de la protección de datos;

(ooo) las garantías de cumplimiento efectivo de la legislación;

(ppp) las disposiciones legislativas en materia de insolvencia que se aplicarían en caso de quiebra del proveedor tercero de servicios de TIC;

(qqq) cualquier restricción que pueda surgir y que afecte a la recuperación urgente de los datos de la entidad financiera.

Las entidades financieras evaluarán si las cadenas de subcontratación potencialmente largas o complejas pueden afectar a su capacidad para efectuar un seguimiento completo de las funciones contratadas y a la capacidad de la autoridad competente para supervisar eficazmente a la entidad financiera a este respecto, y en qué medida.

Artículo 27

Cláusulas contractuales fundamentales

49. Los derechos y obligaciones de la entidad financiera y del proveedor tercero de servicios de TIC estarán claramente asignados y establecidos por escrito. El contrato completo, que incluirá los acuerdos de nivel de servicios, se formalizará en un documento escrito que estará a disposición de las partes en papel o en un formato descargable y accesible.

50. Los acuerdos contractuales sobre el uso de servicios de TIC incluirán, como mínimo, lo siguiente:

(rrr) una descripción clara y completa de todas las funciones y servicios que deba prestar el proveedor tercero de servicios de TIC, indicando si está permitida la subcontratación de funciones esenciales o importantes, o de partes sustanciales de ellas, y, en caso afirmativo, las condiciones aplicables a dicha subcontratación;

(sss) los lugares en los que deberán proporcionarse las funciones y los servicios contratados o subcontratados y en los que deberán tratarse los datos, incluido el lugar de almacenamiento, y el requisito de que el proveedor tercero de servicios de TIC notifique a la entidad financiera cualquier cambio previsto de dichos lugares;

(ttt) disposiciones sobre accesibilidad, disponibilidad, integridad, seguridad y protección de los datos personales y sobre las garantías de la entidad financiera de poder acceder a los datos personales y no personales tratados y poder recuperarlos y que le sean devueltos en un formato fácilmente accesible, en caso de insolvencia, resolución o interrupción de las operaciones comerciales del proveedor tercero de servicios de TIC;

(uuu) descripciones completas del nivel de servicio, incluidas sus actualizaciones y revisiones, y objetivos precisos de rendimiento cuantitativos y cualitativos dentro de los niveles de servicio acordados, de modo que la entidad financiera pueda realizar un seguimiento efectivo y que puedan adoptarse sin demora indebida las medidas correctoras adecuadas cuando no se alcancen los niveles de servicio acordados;

(vvv) plazos de notificación y obligaciones de información del proveedor tercero de servicios de TIC a la entidad financiera, incluida la notificación de cualquier hecho que pueda tener un efecto significativo en la capacidad del proveedor tercero de servicios de TIC para desempeñar eficazmente funciones esenciales o importantes de conformidad con los niveles de servicio acordados;

(www) la obligación del proveedor tercero de servicios de TIC de prestar asistencia en caso de que se produzca un incidente de TIC sin coste adicional o a un coste predeterminado;

(xxx) la obligación de que el proveedor tercero de servicios de TIC aplique y ponga a prueba planes de contingencia empresarial y disponga de medidas, herramientas y políticas de seguridad de las TIC que garanticen suficientemente una prestación de servicios segura por parte de la entidad financiera en consonancia con su marco regulador;

(yyy) el derecho a realizar un seguimiento continuo de la actuación del proveedor tercero de servicios de TIC, lo que incluye:

i) los derechos de acceso, inspección y auditoría por la entidad financiera o por un tercero designado, y el derecho a hacer copias de la documentación pertinente, cuyo ejercicio efectivo no se vea obstaculizado o limitado por otros acuerdos contractuales o políticas de aplicación;

ii) el derecho a acordar niveles de garantía alternativos si se ven afectados los derechos de otros clientes;

iii) el compromiso de cooperar plenamente durante las inspecciones *in situ* realizadas por la entidad financiera y detalles sobre el alcance, las modalidades y la frecuencia de las auditorías a distancia;

(zzz) la obligación del proveedor tercero de servicios de TIC de cooperar plenamente con las autoridades competentes y las autoridades de resolución de la entidad financiera, incluidas las personas designadas por ellas;

(aaaa) los derechos de rescisión y el correspondiente plazo mínimo de preaviso para la rescisión del contrato, de conformidad con las expectativas de las autoridades competentes;

(bbbb) estrategias de salida, en particular el establecimiento de un período transitorio suficiente obligatorio:

(a) durante el cual el proveedor tercero de servicios de TIC seguirá proporcionando las funciones o los servicios de que se trate con el fin de reducir el riesgo de perturbaciones en la entidad financiera;

(b) que permita a la entidad financiera cambiar a otro proveedor tercero de servicios de TIC o adoptar soluciones internas coherentes con la complejidad del servicio prestado.

51. Al negociar acuerdos contractuales, las entidades financieras y los proveedores terceros de servicios de TIC considerarán el uso de cláusulas contractuales tipo elaboradas para servicios específicos.

52. Las AES, a través del Comité Mixto, elaborarán proyectos de normas técnicas de regulación para especificar más detalladamente los elementos que una entidad financiera deberá determinar y evaluar cuando subcontrate funciones esenciales o importantes a fin de dar correcto cumplimiento a lo dispuesto en el apartado 2, letra a).

Las AES presentarán a la Comisión dichos proyectos de normas técnicas de regulación a más tardar [*OP: insértese la fecha correspondiente a 1 año después de la fecha de entrada en vigor*].

Se delegan en la Comisión los poderes para completar el presente Reglamento mediante la adopción de las normas técnicas de regulación a que se refiere el párrafo primero de conformidad con los artículos 10 a 14 del Reglamento (UE) n.º 1093/2010, el Reglamento (UE) n.º 1095/2010 y el Reglamento (UE) n.º 1094/2010.

SECCIÓN II

MARCO DE SUPERVISIÓN DE LOS PROVEEDORES TERCEROS ESENCIALES DE SERVICIOS DE TIC

Artículo 28

Designación de proveedores terceros esenciales de servicios de TIC

53. Las AES, a través del Comité Mixto y por recomendación del Foro de Supervisión establecido de conformidad con el artículo 29, apartado 1, deberán:

(cccc) designar a los proveedores terceros de servicios de TIC que sean esenciales para las entidades financieras, teniendo en cuenta los criterios especificados en el apartado 2;

(dddd) designar a la ABE, la AEVM o la AESPJ como supervisor principal para cada proveedor tercero esencial de servicios de TIC, dependiendo de si el valor total de los activos de las entidades financieras que utilizan los servicios de dicho proveedor tercero esencial de servicios de TIC y que están contempladas en el Reglamento (UE) n.º 1093/2010, el Reglamento (UE) n.º 1094/2010 o el Reglamento (UE) n.º 1095/2010 representa más de la mitad del valor de los activos totales de todas las entidades financieras que utilizan los servicios del proveedor tercero esencial de servicios de TIC, según conste en los balances consolidados o en los balances individuales, cuando no estén consolidados, de dichas entidades financieras.

54. La designación a que se refiere el apartado 1, letra a), se basará en todos los criterios siguientes:

(eeee) el efecto sistémico en la estabilidad, la continuidad o la calidad de la prestación de servicios financieros de un posible fallo operativo a gran escala del proveedor tercero de TIC de que se trate que afecte a la prestación de sus servicios, teniendo en cuenta el número de entidades financieras a las que presta servicios dicho proveedor;

(ffff) el carácter o la importancia sistémicos de las entidades financieras que dependen del proveedor tercero de TIC de que se trate, evaluados con arreglo a los parámetros siguientes:

i) el número de entidades de importancia sistémica mundial (EISM) u otras entidades de importancia sistémica (OEIS) que dependen del proveedor tercero de servicios de TIC correspondiente;

ii) la interdependencia entre las EISM u OEIS a que se refiere el inciso i) y otras entidades financieras, incluidas las situaciones en las que las EISM u OEIS prestan servicios de infraestructura financiera a otras entidades financieras;

(gggg) la dependencia de las entidades financieras respecto de los servicios prestados por el proveedor tercero de servicios de TIC pertinente en relación con funciones esenciales o importantes de entidades financieras que, en última instancia, impliquen al mismo proveedor tercero de servicios de TIC, con independencia de que las entidades financieras recurran a dichos servicios directa o indirectamente, por medio o a través de acuerdos de subcontratación;

(hhhh) el grado de sustituibilidad del proveedor tercero de servicios de TIC, teniendo en cuenta los parámetros siguientes:

i) la falta de alternativas reales, siquiera parciales, debido al número limitado de proveedores terceros de servicios de TIC activos en un mercado específico, o a la cuota de mercado del proveedor tercero de servicios de TIC de que se trate, o a la complejidad o dificultad técnica existente, entre otras cosas en relación con tecnologías protegidas por derechos, o a las características específicas de la organización o la actividad del proveedor tercero de servicios de TIC;

ii) las dificultades para efectuar la migración parcial o total de los datos y cargas de trabajo pertinentes del proveedor tercero de servicios de TIC considerado a otro, al ser significativos los costes financieros, el tiempo u otro tipo de recursos que el proceso de migración podría implicar, o debido al aumento de los riesgos de TIC u otros riesgos operativos a los que podría verse expuesta la entidad financiera a través de dicha migración;

(iiii) el número de Estados miembros en los que presta servicios el proveedor tercero de servicios de TIC de que se trate;

(jjjj) el número de Estados miembros en los que operan las entidades financieras que recurren al proveedor tercero de servicios de TIC de que se trate.

55. Se otorgan a la Comisión los poderes para adoptar actos delegados, de conformidad con el artículo 50, que completen los criterios mencionados en el apartado 2.

56. El mecanismo de designación a que se refiere el apartado 1, letra a), no se utilizará hasta que la Comisión haya adoptado un acto delegado de conformidad con el apartado 3.

57. El mecanismo de designación a que se refiere el apartado 1, letra a), no se aplicará en relación con los proveedores terceros de servicios de TIC que estén sujetos a marcos de supervisión establecidos en apoyo de las tareas a que se refiere el artículo 127, apartado 2, del Tratado de Funcionamiento de la Unión Europea.

58. Las AES, a través del Comité Mixto, establecerán, publicarán y actualizarán anualmente la lista de proveedores terceros esenciales de servicios de TIC en la Unión.

59. A efectos de lo dispuesto en el apartado 1, letra a), las autoridades competentes transmitirán anualmente y de forma agregada los informes a que se refiere el artículo 25, apartado 4, al Foro de Supervisión establecido de conformidad con el artículo 29. El Foro de Supervisión evaluará las dependencias de las entidades financieras respecto de terceros en lo que respecta a las TIC con arreglo a la información recibida de las autoridades competentes.

60. Los proveedores terceros de servicios de TIC que no estén incluidos en la lista a que se refiere el apartado 6 podrán solicitar ser incluidos en dicha lista.

A efectos de lo dispuesto en el párrafo primero, el proveedor tercero de servicios de TIC presentará una solicitud motivada a la ABE, la AEVM o la AESPJ, que, a través del Comité Mixto, decidirán si lo incluyen o no en esa lista de conformidad con el apartado 1, letra a).

La decisión a que se refiere el párrafo segundo se adoptará y notificará al proveedor tercero de servicios de TIC en un plazo de seis meses a partir de la recepción de la solicitud.

61. Las entidades financieras no recurrirán a un proveedor tercero de servicios de TIC establecido en un tercer país que sería designado como esencial con arreglo al apartado 1, letra a), si estuviera establecido en la Unión.

Artículo 29

Estructura del marco de supervisión

62. El Comité Mixto, de conformidad con el artículo 57 del Reglamento (UE) n.º 1093/2010, el Reglamento (UE) n.º 1094/2010 y el Reglamento (UE) n.º 1095/2010, establecerá el Foro de Supervisión como subcomité encargado de apoyar el trabajo del Comité Mixto y del supervisor principal a que se refiere el artículo 28, apartado 1, letra b), en materia de riesgo de terceros relacionado con las TIC en los distintos sectores financieros. El Foro de Supervisión preparará los proyectos de posiciones conjuntas y actos comunes del Comité Mixto en este ámbito.

El Foro de Supervisión debatirá periódicamente las novedades pertinentes en materia de riesgos y vulnerabilidades de las TIC y promoverá un enfoque coherente de seguimiento de los riesgos de terceros relacionados con las TIC a nivel de la Unión.

63. El Foro de Supervisión llevará a cabo anualmente una evaluación colectiva de los resultados y las conclusiones de las actividades de supervisión realizadas para todos los proveedores terceros esenciales de TIC y promoverá medidas de coordinación para incrementar la resiliencia operativa digital de las entidades financieras, fomentar buenas prácticas para hacer frente al riesgo de concentración de TIC y estudiar medidas de mitigación de la transferencia de riesgos entre sectores.

64. El Foro de Supervisión presentará parámetros de referencia exhaustivos respecto de los proveedores terceros esenciales de servicios de TIC, que el Comité Mixto adoptará como posiciones conjuntas de las AES de conformidad con el artículo 56, apartado 1, del Reglamento (UE) n.º 1093/2010, del Reglamento (UE) n.º 1094/2010 y del Reglamento (UE) n.º 1095/2010.

65. El Foro de Supervisión estará integrado por los presidentes de las AES y un representante de alto nivel del personal en ejercicio de la autoridad competente pertinente de cada Estado miembro. Los respectivos directores ejecutivos de cada AES y un representante de la Comisión Europea, de la JERS, del BCE y de la ENISA participarán en el Foro de Supervisión en calidad de observadores.

66. De conformidad con el artículo 16 del Reglamento (UE) n.º 1093/2010, del Reglamento (UE) n.º 1094/2010 y del Reglamento (UE) n.º 1095/2010, las AES emitirán directrices sobre la cooperación entre ellas y las autoridades competentes a efectos de lo dispuesto en la presente sección sobre los procedimientos y las condiciones detallados relativos a la ejecución de las tareas entre las autoridades competentes y las AES, así como los pormenores sobre los intercambios de información que necesiten las autoridades competentes para garantizar el cumplimiento de las recomendaciones formuladas por los supervisores principales de conformidad con el artículo 31, apartado 1, letra d), a los proveedores terceros esenciales de TIC.

67. Los requisitos establecidos en la presente sección se entenderán sin perjuicio de la aplicación de la Directiva (UE) 2016/1148 y de otras normas de la Unión sobre supervisión aplicables a los proveedores de servicios de computación en nube.

68. Las AES, a través del Comité Mixto y basándose en los trabajos preparatorios realizados por el Foro de Supervisión, presentarán anualmente al Parlamento Europeo, al Consejo y a la Comisión un informe sobre la aplicación de la presente sección.

Artículo 30

Tareas del supervisor principal

69. El supervisor principal evaluará si cada proveedor tercero de servicios de TIC esencial ha establecido normas, procedimientos, mecanismos y disposiciones completos, sólidos y eficaces para gestionar los riesgos de TIC que pueda plantear a las entidades financieras.

70. La evaluación a la que se refiere el apartado 1 incluirá:

(kkkk) requisitos de las TIC para garantizar, en particular, la seguridad, la disponibilidad, la continuidad, la escalabilidad y la calidad de los servicios que el proveedor tercero esencial de servicios de TIC presta a las entidades financieras, así como la capacidad para mantener en todo momento unos niveles elevados de seguridad, confidencialidad e integridad de los datos;

(llll) la seguridad física que contribuye a garantizar la seguridad de las TIC, incluida la seguridad de los locales, instalaciones y centros de datos;

(mmmm) los procesos de gestión de riesgos, incluidas las políticas de gestión del riesgo de TIC y los planes de continuidad de la actividad de TIC y de recuperación en caso de catástrofe relacionada con las TIC;

(nnnn) los mecanismos de gobernanza, incluida una estructura organizativa con líneas de responsabilidad claras, transparentes y coherentes y normas de rendición de cuentas que permitan una gestión eficaz del riesgo de TIC;

(oooo) la determinación, el seguimiento y la rápida notificación a las entidades financieras de los incidentes relacionados con las TIC, la gestión y la resolución de dichos incidentes, en particular de los ciberataques;

(pppp) los mecanismos para la portabilidad de los datos y la portabilidad e interoperabilidad de las aplicaciones, que garanticen el ejercicio efectivo de los derechos de rescisión por las entidades financieras;

(qqqq) la puesta a prueba de los sistemas, las infraestructuras y los controles de TIC;

(rrrr) las auditorías de TIC;

(ssss) el uso de los estándares nacionales e internacionales pertinentes aplicables a la prestación de sus servicios de TIC a las entidades financieras.

71. Sobre la base de la evaluación a que se refiere el apartado 1, el supervisor principal adoptará un plan de supervisión individual claro, detallado y motivado para cada proveedor tercero esencial de servicios de TIC. Dicho plan se comunicará cada año al proveedor tercero esencial de servicios de TIC.

72. Una vez que los planes de supervisión anuales a que se refiere el apartado 3 hayan sido acordados y notificados a los proveedores terceros esenciales de servicios de TIC, las autoridades competentes solo podrán adoptar medidas en relación con dichos proveedores de acuerdo con el supervisor principal.

Artículo 31

Facultades del supervisor principal

73. A efectos del desempeño de las obligaciones establecidas en la presente sección, el supervisor principal dispondrá de las siguientes facultades:

(tttt) solicitar toda la información y la documentación pertinentes de conformidad con el artículo 32;

(uuuu) llevar a cabo investigaciones generales e inspecciones de conformidad con los artículos 33 y 34;

(vvvv) una vez finalizadas las actividades de supervisión, solicitar informes en los que se especifiquen las medidas adoptadas o las correcciones aplicadas por los proveedores terceros esenciales de TIC en relación con las recomendaciones a que se refiere la letra d) del presente apartado;

(wwww) formular recomendaciones sobre los ámbitos a los que se refiere el artículo 30, apartado 2, en particular en relación con lo siguiente:

i) la aplicación de requisitos o procesos específicos de seguridad y calidad de las TIC, en particular en relación con la instalación de parches, actualizaciones, cifrado y otras medidas de seguridad que el supervisor principal considere pertinentes para garantizar la seguridad, desde el punto de vista de las TIC, de los servicios prestados a las entidades financieras;

ii) la aplicación de condiciones, incluida su ejecución técnica, a las que deba ajustarse la prestación de servicios a las entidades financieras por los proveedores terceros esenciales de servicios de TIC, y que el supervisor principal considere pertinentes para impedir que se generen o se amplíen puntos únicos de fallo, o para minimizar el posible impacto sistémico en el sector financiero de la Unión en caso de riesgo de concentración de TIC;

iii) tras el examen realizado de conformidad con los artículos 32 y 33 de los acuerdos de subcontratación, incluidos los acuerdos de subexternalización que los proveedores terceros esenciales de servicios de TIC prevean celebrar con otros proveedores terceros de servicios de TIC o con subcontratistas de TIC establecidos en un tercer país, cualquier subcontratación prevista, incluida la subexternalización, cuando el supervisor principal considere que toda ulterior subcontratación puede ocasionar riesgos para la prestación de servicios por la entidad financiera, o riesgos para la estabilidad financiera;

iv) abstenerse de celebrar un acuerdo adicional de subcontratación, cuando se cumplan todas las condiciones siguientes:

– que el subcontratista previsto sea un proveedor tercero de servicios de TIC o un subcontratista de TIC establecido en un tercer país;

– que la subcontratación se refiera a una función esencial o importante de la entidad financiera.

74. El supervisor principal consultará al Foro de Supervisión antes de ejercer las facultades a que se refiere el apartado 1.

75. Los proveedores terceros esenciales de servicios de TIC cooperarán de buena fe con el supervisor principal y le asistirán en el desempeño de sus tareas.

76. El supervisor principal podrá imponer una multa coercitiva para obligar al proveedor tercero esencial de servicios de TIC a cumplir lo dispuesto en el apartado 1, letras a), b) y c).

77. La multa coercitiva a que se refiere el apartado 4 se impondrá diariamente hasta que se logre el cumplimiento y por un período máximo de seis meses a partir de la notificación al proveedor tercero esencial de servicios de TIC.

78. El importe de la multa coercitiva, calculado a partir de la fecha establecida en la decisión por la que se imponga dicha multa, será del 1 % del volumen de negocios diario medio a escala mundial del proveedor tercero esencial de servicios de TIC en el ejercicio precedente.

79. Las multas coercitivas serán de carácter administrativo y tendrán fuerza ejecutiva. La ejecución forzosa se regirá por las normas de procedimiento civil vigentes en el Estado miembro en cuyo territorio se lleven a cabo las inspecciones y el acceso. Los órganos jurisdiccionales del Estado miembro de que se trate serán competentes para conocer de las denuncias relacionadas con irregularidades en la ejecución. Los importes de las multas coercitivas se asignarán al presupuesto general de la Unión Europea.

80. Las AES harán públicas todas las multas coercitivas que se impongan, a menos que dicha divulgación pusiera en grave riesgo los mercados financieros o causara un perjuicio desproporcionado a las partes implicadas.

81. Antes de imponer una multa coercitiva de conformidad con el apartado 4, el supervisor principal ofrecerá a los representantes del proveedor tercero esencial de TIC objeto del procedimiento la oportunidad de ser oídos en relación con sus conclusiones y basará sus decisiones únicamente en las conclusiones acerca de las cuales el proveedor tercero esencial de TIC haya tenido la oportunidad de formular observaciones. Los derechos de defensa de las personas objeto del procedimiento estarán garantizados plenamente en el curso del procedimiento. Dichas personas tendrán derecho a acceder al expediente, sin perjuicio de los intereses legítimos de protección de los secretos comerciales de terceros. El derecho de acceso al expediente no se extenderá a la información confidencial ni a los documentos preparatorios internos del supervisor principal.

Artículo 32
Solicitud de información

82. El supervisor principal, mediante simple solicitud o mediante decisión, podrá instar a los proveedores terceros esenciales de TIC a que faciliten cuanta información le sea necesaria para desempeñar sus obligaciones con arreglo al presente Reglamento, incluidos todos los documentos comerciales u operativos, contratos, documentación sobre políticas, informes de auditoría de seguridad de las TIC e informes sobre incidentes relacionados con las TIC pertinentes, así como cualquier información relativa a las partes a las que el proveedor tercero esencial de TIC haya externalizado funciones o actividades operativas.

83. Al enviar una simple solicitud de información con arreglo al apartado 1, el supervisor principal:

(xxxx) hará referencia al presente artículo como base jurídica de la solicitud;

(yyyy) indicará el propósito de la solicitud;

(zzzz)especificará la información requerida;

(aaaaa) fijará el plazo en el que habrá de serle facilitada la información;

(bbbbb) informará al representante del proveedor tercero esencial de servicios de TIC al que se solicite la información de que no está obligado a facilitar esa información, pero, en caso de que acceda voluntariamente a hacerlo, la información que facilite no deberá ser incorrecta ni engañosa.

84. Cuando exija que se facilite información con arreglo al apartado 1, el supervisor principal:

(ccccc) hará referencia al presente artículo como base jurídica de la solicitud;

(ddddd) indicará el propósito de la solicitud;

(eeeee) especificará la información requerida;

(fffff)fijará el plazo en el que habrá de serle facilitada la información;

(ggggg) indicará las multas coercitivas previstas en el artículo 31, apartado 4, en caso de que no se facilite toda la información exigida;

(hhhhh) hará constar el derecho de recurrir la decisión ante la Sala de Recurso de la AES y ante el Tribunal de Justicia de la Unión Europea (en lo sucesivo «el Tribunal de Justicia»), de conformidad con los artículos 60 y 61 del

Reglamento (UE) n.º 1093/2010, del Reglamento (UE) n.º 1094/2010 y del Reglamento (UE) n.º 1095/2010.

85. Los representantes de proveedores terceros esenciales de servicios de TIC facilitarán la información solicitada. Los abogados debidamente habilitados podrán facilitar la información en nombre de sus representados. El proveedor tercero esencial de servicios de TIC seguirá siendo plenamente responsable si la información suministrada es incompleta, incorrecta o engañosa.

86. El supervisor principal enviará sin demora una copia de la decisión de facilitar información a las autoridades competentes de las entidades financieras que utilicen los servicios del proveedor tercero esencial de TIC.

Artículo 33
Investigaciones generales

87. A fin de desempeñar sus obligaciones con arreglo al presente Reglamento, el supervisor principal, asistido por el equipo de examen a que se refiere el artículo 34, apartado 1, podrá llevar a cabo las investigaciones necesarias de proveedores terceros de servicios de TIC.

88. El supervisor principal estará facultado para:

(iiiii) examinar los registros, datos, procedimientos y cualquier otra documentación pertinente para la realización de su cometido, independientemente del medio utilizado para almacenarlos;

(jjjjj) hacer u obtener copias certificadas o extractos de dichos registros, datos, procedimientos y otra documentación;

(kkkkk) convocar a los representantes del proveedor tercero de servicios de TIC para que den explicaciones orales o escritas sobre los hechos o documentos que guarden relación con el objeto y el propósito de la investigación, y registrar las respuestas;

(lllll) entrevistar a cualquier otra persona física o jurídica que acepte ser entrevistada a fin de recabar información relacionada con el objeto de una investigación;

(mmmmm) requerir una relación de comunicaciones telefónicas y tráfico de datos.

89. Los agentes y demás personas acreditadas por el supervisor principal para realizar la investigación a que se refiere el apartado 1 ejercerán sus facultades previa presentación de una autorización escrita que especifique el objeto y el propósito de la investigación.

Dicha autorización indicará asimismo las multas coercitivas previstas en el artículo 31, apartado 4, cuando los registros, datos, procedimientos o cualquier otra documentación exigida, o las respuestas a las preguntas formuladas a los representantes del proveedor tercero de servicios de TIC, no se faciliten o sean incompletos.

90. Los representantes de los proveedores terceros de servicios de TIC estarán obligados a someterse a las investigaciones sobre la base de una decisión del supervisor principal. La decisión precisará el objeto y el propósito de la investigación, las multas coercitivas previstas en el artículo 31, apartado 4, las vías de recurso posibles con arreglo al Reglamento (UE) n.º 1093/2010, al Reglamento (UE) n.º 1094/2010 y

al Reglamento (UE) n.º 1095/2010, así como el derecho a recurrir la decisión ante el Tribunal de Justicia.

91. El supervisor principal informará, con suficiente antelación, de la investigación y de la identidad de las personas acreditadas a las autoridades competentes de las entidades financieras que recurran a ese proveedor tercero de servicios de TIC.

Artículo 34
Inspecciones in situ

92. A fin de desempeñar sus obligaciones con arreglo al presente Reglamento, el supervisor principal, asistido por los equipos de examen a que se refiere el artículo 35, apartado 1, podrá acceder a cualquier local comercial, terreno o propiedad de proveedores terceros de TIC, como sedes centrales, centros de operaciones y locales secundarios, y realizar todas las inspecciones *in situ* que sean necesarias, así como realizar inspecciones fuera de línea.

93. Los agentes y demás personas acreditadas por el supervisor principal para llevar a cabo una inspección *in situ* podrán acceder a cualquiera de dichos locales comerciales, terrenos o propiedades y tendrán plenas facultades para precintar cualesquiera locales comerciales y libros o registros por el tiempo que dure la inspección y en la medida en que sea necesario para esta.

Ejercerán sus facultades previa presentación de una autorización escrita en la que se especifiquen el objeto y el propósito de la inspección y las multas coercitivas previstas en el artículo 31, apartado 4, cuando los representantes de los proveedores terceros de servicios de TIC de que se trate no se sometan a la inspección.

94. El supervisor principal informará con suficiente antelación de la inspección a las autoridades competentes de las entidades financieras que recurran a ese proveedor tercero de TIC.

95. Las inspecciones abarcarán todo el conjunto de sistemas, redes, dispositivos, información y datos de TIC pertinentes utilizados para la prestación de servicios a las entidades financieras o que contribuyan a ella.

96. Antes de cualquier visita *in situ* prevista, los supervisores principales avisarán con una antelación razonable a los proveedores terceros esenciales de servicios de TIC, a menos que dicho aviso no sea posible debido a una situación de emergencia o de crisis, o a que conduzca a una situación en la que la inspección o la auditoría dejarían de ser eficaces.

97. El proveedor tercero esencial de servicios de TIC se someterá a las inspecciones *in situ* ordenadas mediante decisión del supervisor principal. La decisión especificará el objeto y el propósito de la inspección, fijará la fecha de su comienzo e indicará las multas coercitivas previstas en el artículo 31, apartado 4, las vías de recurso posibles con arreglo al Reglamento (UE) n.º 1093/2010, al Reglamento (UE) n.º 1094/2010 y al Reglamento (UE) n.º 1095/2010, así como el derecho a recurrir la decisión ante el Tribunal de Justicia.

98. En caso de que los agentes y demás personas acreditadas por el supervisor principal constaten que un proveedor tercero esencial de servicios de TIC se opone a una inspección ordenada conforme al presente artículo, el supervisor principal informará al proveedor esencial de servicios de TIC de las consecuencias de dicha oposición, incluida la posibilidad de que las autoridades competentes de las entidades

financieras pertinentes pongan fin a los acuerdos contractuales celebrados con dicho proveedor.

Artículo 35

Supervisión permanente

99. Cuando lleven a cabo investigaciones generales o inspecciones *in situ*, los supervisores principales estarán asistidos por un equipo de examen establecido para cada proveedor tercero esencial de servicios de TIC.

100. El equipo de examen conjunto a que se refiere el apartado 1 estará compuesto por miembros del personal del supervisor principal y de las autoridades competentes pertinentes que supervisen a las entidades financieras a las que preste servicios el proveedor tercero esencial de servicios de TIC, que participarán en la preparación y ejecución de las actividades de supervisión, y constará de un máximo de diez miembros. Todos los miembros del equipo de examen conjunto deberán tener experiencia en materia de riesgo de TIC y riesgo operativo. El equipo de examen conjunto trabajará bajo la coordinación de un miembro del personal de la AES designado (el «coordinador del supervisor principal»).

101. Las AES, a través del Comité Mixto, elaborarán proyectos de normas técnicas de regulación comunes para especificar más detalladamente la designación de los miembros del equipo de examen conjunto procedentes de las autoridades competentes pertinentes, así como las tareas y las modalidades de trabajo del equipo de examen. Las AES presentarán a la Comisión dichos proyectos de normas técnicas de regulación a más tardar [*PO: insértese la fecha correspondiente a 1 año después de la fecha de entrada en vigor*].

Se delegan en la Comisión los poderes para adoptar las normas técnicas de regulación a que se refiere el párrafo primero de conformidad con los artículos 10 a 14 del Reglamento (UE) n.º 1093/2010, el Reglamento (UE) n.º 1094/2010 y el Reglamento (UE) n.º 1095/2010.

102. En los tres meses siguientes a la conclusión de una investigación o una inspección *in situ*, el supervisor principal, previa consulta al Foro de Supervisión, adoptará las recomendaciones que formulará al proveedor tercero esencial de servicios de TIC en virtud de las facultades a que se refiere el artículo 31.

103. Las recomendaciones a las que se refiere el apartado 4 se comunicarán inmediatamente al proveedor tercero esencial de servicios de TIC y a las autoridades competentes de las entidades financieras a las que preste servicios.

Para llevar a cabo las actividades de supervisión, los supervisores principales podrán tener en cuenta las certificaciones de terceros pertinentes y los informes de auditoría interna o externa de terceros proveedores de TIC facilitados por el proveedor tercero esencial de servicios de TIC.

Artículo 36

Armonización de las condiciones que permiten llevar a cabo la supervisión

104. Las AES, a través del Comité Mixto, elaborarán proyectos de normas técnicas de regulación para especificar:

(nnnnn) la información que debe facilitar un proveedor tercero esencial de servicios de TIC en la solicitud de inclusión voluntaria contemplada en el artículo 28, apartado 8;

(ooooo) el contenido y el formato de los informes que pueden solicitarse a efectos del artículo 31, apartado 1, letra c);

(ppppp) la presentación de la información, incluidos la estructura, los formatos y los métodos que un proveedor tercero esencial de servicios de TIC deberá presentar, divulgar o notificar de conformidad con el artículo 31, apartado 1;

(qqqqq) los pormenores de la evaluación por las autoridades competentes de las medidas adoptadas por los proveedores terceros esenciales de servicios de TIC en aplicación de las recomendaciones de los supervisores principales con arreglo al artículo 37, apartado 2.

105. Las AES presentarán a la Comisión dichos proyectos de normas técnicas de regulación a más tardar el 1 de enero de 20xx [*OP: insértese la fecha correspondiente a 1 año después de la fecha de entrada en vigor*].

Se delegan en la Comisión los poderes para completar el presente Reglamento mediante la adopción de las normas técnicas de regulación a que se refiere el párrafo primero de conformidad con el procedimiento establecido en los artículos 10 a 14 del Reglamento (UE) n.º 1093/2010, el Reglamento (UE) n.º 1094/2010 y el Reglamento (UE) n.º 1095/2010.

Artículo 37

Seguimiento por las autoridades competentes

106. En el plazo de treinta días naturales a partir de la recepción de las recomendaciones emitidas por los supervisores principales de conformidad con el artículo 31, apartado 1, letra d), los proveedores terceros esenciales de servicios de TIC notificarán al supervisor principal si tienen intención de seguir dichas recomendaciones. Los supervisores principales transmitirán inmediatamente esta información a las autoridades competentes.

107. Las autoridades competentes comprobarán si las entidades financieras tienen en cuenta los riesgos señalados en las recomendaciones dirigidas por el supervisor principal a los proveedores terceros esenciales de TIC de conformidad con el artículo 31, apartado 1, letra d).

108. Las autoridades competentes podrán, de conformidad con el artículo 44, exigir a las entidades financieras que suspendan temporalmente, de manera parcial o total, el uso o la implantación de un servicio prestado por el proveedor tercero esencial de TIC hasta que se hayan subsanado los riesgos mencionados en las recomendaciones dirigidas a los proveedores terceros esenciales de TIC. En caso necesario, podrán exigir a las entidades financieras que pongan fin, en parte o en su totalidad, a los acuerdos contractuales pertinentes celebrados con los proveedores terceros esenciales de servicios de TIC.

109. Al adoptar las decisiones a que se refiere el apartado 3, las autoridades competentes tendrán en cuenta el tipo y la magnitud del riesgo no subsanado por el proveedor tercero esencial de servicios de TIC, así como la gravedad del incumplimiento, considerando los siguientes criterios:

(rrrrr)la gravedad y la duración del incumplimiento;

(sssss) si el incumplimiento ha puesto de manifiesto deficiencias graves en los procedimientos, los sistemas de gestión, la gestión de riesgos y los controles internos del proveedor tercero esencial de servicios de TIC;

(ttttt) si el incumplimiento ha facilitado, provocado o contribuido de cualquier otro modo a la comisión de un delito financiero;

(uuuuu) si el incumplimiento ha sido cometido con dolo o por negligencia.

110. Las autoridades competentes informarán periódicamente a los supervisores principales sobre los enfoques y las medidas adoptados en el desempeño de sus tareas de supervisión en relación con las entidades financieras, así como sobre las medidas contractuales adoptadas por estas cuando los proveedores terceros esenciales de servicios de TIC no hayan observado en parte o en su totalidad las recomendaciones formuladas por los supervisores principales.

Artículo 38
Tasas de supervisión

111. Las AES cobrarán a los proveedores terceros esenciales de servicios de TIC unas tasas que cubran por completo los gastos que deban asumir las AES para la realización de las tareas de supervisión de conformidad con el presente Reglamento, incluido el reembolso de los costes que puedan derivarse del trabajo realizado por las autoridades competentes que participen en las actividades de supervisión de conformidad con el artículo 35.

El importe de las tasas cobradas a un proveedor tercero esencial de servicios de TIC cubrirá todos los costes administrativos y será proporcional a su volumen de negocios.

112. Se otorgan a la Comisión los poderes para adoptar un acto delegado con arreglo al artículo 50 por el que se complete el presente Reglamento mediante la determinación del importe de las tasas y las modalidades de pago.

Artículo 39
Cooperación internacional

113. La ABE, la AEVM y la AESPJ podrán, de conformidad con el artículo 33 del Reglamento (UE) n.º 1093/2010, del Reglamento (UE) n.º 1094/2010 y del Reglamento (UE) n.º 1095/2010, celebrar acuerdos administrativos con las autoridades de regulación y supervisión de terceros países para fomentar la cooperación internacional en materia de riesgo de terceros relacionado con las TIC en diferentes sectores financieros, en particular mediante el desarrollo de buenas prácticas para la evaluación de las prácticas y controles de gestión del riesgo de TIC, las medidas de mitigación y las respuestas a los incidentes.

114. Las AES, a través del Comité Mixto, presentarán cada cinco años al Parlamento Europeo, al Consejo y a la Comisión un informe confidencial conjunto en el que se resuman las conclusiones de los debates pertinentes mantenidos con las autoridades de terceros países a que se refiere el apartado 1, centrándose en la evolución del riesgo de terceros relacionado con las TIC y sus implicaciones para la estabilidad financiera, la integridad del mercado, la protección de los inversores o el funcionamiento del mercado único.

CAPÍTULO VI

ACUERDOS DE INTERCAMBIO DE INFORMACIÓN

Artículo 40

Acuerdos de intercambio de información en relación con información e inteligencia sobre ciberamenazas

115. Las entidades financieras podrán intercambiar entre sí información e inteligencia sobre ciberamenazas, incluidos indicadores de compromiso, tácticas, técnicas y procedimientos, alertas de ciberseguridad y herramientas de configuración, en la medida en que dicho intercambio de información e inteligencia:

(vvvvv) tenga por objeto mejorar la resiliencia operativa digital de las entidades financieras, en particular mediante la sensibilización en relación con las ciberamenazas, la limitación o la desactivación de la capacidad de propagación de las ciberamenazas, el apoyo a la gama de capacidades defensivas, las técnicas de detección de amenazas, las estrategias de mitigación o las fases de respuesta y recuperación de las entidades financieras;

(wwwww) tenga lugar dentro de comunidades de entidades financieras de confianza;

(xxxxx) se realice mediante acuerdos de intercambio de información que protejan el carácter potencialmente sensible de la información compartida y se rijan por normas de conducta que respeten plenamente el secreto comercial, la protección de los datos personales[48] y las directrices sobre política de competencia[49].

116. A efectos de lo dispuesto en el apartado 1, letra c), en los acuerdos de intercambio de información se definirán las condiciones de participación y, cuando proceda, se establecerán los detalles relativos a la participación de las autoridades públicas y a la calidad en la que estas podrán asociarse a ellos, así como los detalles sobre los elementos operativos, incluido el uso de plataformas informáticas especializadas.

117. Las entidades financieras notificarán a las autoridades competentes su participación en los acuerdos de intercambio de información a que se refiere el apartado 1, en el momento en que se valide su incorporación a ellos o, en su caso, el cese de su participación, una vez que este se haga efectivo.

CAPÍTULO VII

AUTORIDADES COMPETENTES

[48] De conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) (DO L 119 de 4.5.2016, p. 1).

[49] Comunicación de la Comisión «Directrices sobre la aplicabilidad del artículo 101 del Tratado de Funcionamiento de la Unión Europea a los acuerdos de cooperación horizontal» (DO C 11 de 14.1.2011, p. 1).

Artículo 41

Autoridades competentes

Sin perjuicio de las disposiciones relativas al marco de supervisión de los proveedores terceros esenciales de servicios de TIC a que se refiere el capítulo V, sección II, del presente Reglamento, el cumplimiento de las obligaciones establecidas en el presente Reglamento será garantizado por las siguientes autoridades competentes de conformidad con las facultades otorgadas por los respectivos actos jurídicos:

(yyyyy) en lo que respecta a las entidades de crédito, la autoridad competente designada de conformidad con el artículo 4 de la Directiva 2013/36/UE, sin perjuicio de las tareas específicas que el Reglamento (UE) n.º 1024/2013 encomienda al BCE;

(zzzzz) en lo que respecta a los proveedores de servicios de pago, la autoridad competente designada de conformidad con el artículo 22 de la Directiva (UE) 2015/2366;

(aaaaaa) en lo que respecta a las entidades de dinero electrónico, la autoridad competente designada con arreglo al artículo 37 de la Directiva 2009/110/CE;

(bbbbbb) en lo que respecta a las empresas de servicios de inversión, la autoridad competente designada de conformidad con el artículo 4 de la Directiva (UE) 2019/2034;

(cccccc) en lo que respecta a los proveedores de servicios de criptoactivos, los emisores de criptoactivos, los emisores de fichas referenciadas a activos y los emisores de fichas significativas referenciadas a activos, la autoridad competente designada de conformidad con el artículo 3, apartado 1, letra ee), primer guion, del [Reglamento (UE) 20xx Reglamento MICA];

(dddddd) en lo que respecta a los depositarios centrales de valores, la autoridad competente designada de conformidad con el artículo 11 del Reglamento (UE) n.º 909/2014;

(eeeeee) en lo que respecta a las entidades de contrapartida central, la autoridad competente designada de conformidad con el artículo 22 del Reglamento (UE) n.º 648/2012;

(ffffff) en lo que respecta a los centros de negociación y los proveedores de servicios de suministro de datos, la autoridad competente designada de conformidad con el artículo 67 de la Directiva 2014/65/UE;

(gggggg) en lo que respecta a los registros de operaciones, la autoridad competente designada de conformidad con el artículo 55 del Reglamento (UE) n.º 648/2012;

(hhhhhh) en lo que respecta a los gestores de fondos de inversión alternativos, la autoridad competente designada de conformidad con el artículo 44 de la Directiva 2011/61/UE;

(iiiiii) en lo que respecta a las sociedades de gestión, la autoridad competente designada de conformidad con el artículo 97 de la Directiva 2009/65/CE;

(jjjjjj) en lo que respecta a las empresas de seguros y de reaseguros, la autoridad competente designada de conformidad con el artículo 30 de la Directiva 2009/138/CE;

(kkkkkk) en lo que respecta a los intermediarios de seguros, de reaseguros y de seguros complementarios, la autoridad competente designada de conformidad con el artículo 12 de la Directiva (UE) 2016/97;

(llllll) en lo que respecta a los fondos de pensiones de empleo, la autoridad competente designada de conformidad con el artículo 47 de la Directiva 2016/2341;

(mmmmmm) en lo que respecta a las agencias de calificación crediticia, la autoridad competente designada de conformidad con el artículo 21 del Reglamento (CE) n.º 1060/2009;

(nnnnnn) en lo que respecta a los auditores legales y las sociedades de auditoría, la autoridad competente designada de conformidad con el artículo 3, apartado 2, y el artículo 32 de la Directiva 2006/43/CE;

(oooooo) en lo que respecta a los administradores de índices de referencia cruciales, la autoridad competente designada de conformidad con los artículos 40 y 41 del *Reglamento xx/202x*;

(pppppp) en lo que respecta a los proveedores de servicios de financiación participativa, la autoridad competente designada de conformidad con el *artículo x del Reglamento xx/202x*;

(qqqqqq) en lo que respecta a los registros de titulizaciones, la autoridad competente designada de conformidad con el artículo 10 y el artículo 14, apartado 1, del Reglamento (UE) 2017/2402.

Artículo 42

Cooperación con las estructuras y autoridades establecidas por la Directiva (UE) 2016/1148

118. A fin de fomentar la cooperación y permitir los intercambios en materia de supervisión entre las autoridades competentes designadas de conformidad con el presente Reglamento y el Grupo de cooperación establecido por el artículo 11 de la Directiva (UE) 2016/1148, las AES y las autoridades competentes podrán solicitar ser invitadas a los trabajos del Grupo de cooperación.

119. Cuando proceda, las autoridades competentes podrán consultar al punto de contacto único y a los equipos de respuesta a incidentes de seguridad informática nacionales a que se refieren, respectivamente, los artículos 8 y 9 de la Directiva (UE) 2016/1148.

Artículo 43

Ejercicios, comunicación y cooperación intersectoriales en el ámbito financiero

120. Las AES, a través del Comité Mixto y en colaboración con las autoridades competentes, el BCE y la JERS, podrán establecer mecanismos que permitan compartir prácticas eficaces en todos los sectores financieros a fin de mejorar la conciencia situacional y detectar las vulnerabilidades y los riesgos cibernéticos comunes a los diversos sectores.

Podrán organizar ejercicios de gestión de crisis y contingencia que incluyan escenarios de ciberataques con el fin de desarrollar los canales de comunicación y hacer posible gradualmente una respuesta coordinada eficaz a nivel de la UE en caso de que se produzca un incidente grave relacionado con las TIC de alcance

transfronterizo o una amenaza conexa que tenga un impacto sistémico en el sector financiero de la Unión en su conjunto.

Estos ejercicios también podrán poner a prueba, cuando proceda, las dependencias del sector financiero con respecto a otros sectores económicos.

121. Las autoridades competentes, la ABE, la AEVM o la AESPJ, y el BCE cooperarán estrechamente entre sí e intercambiarán información para el desempeño de sus obligaciones de conformidad con los artículos 42 a 48. Coordinarán estrechamente sus actividades de supervisión con el fin de detectar y subsanar las infracciones del presente Reglamento, establecer y promover buenas prácticas, facilitar la colaboración, fomentar la coherencia en la interpretación y proporcionar evaluaciones transterritoriales en caso de desacuerdo.

Artículo 44

Sanciones administrativas y medidas correctoras

122. Las autoridades competentes dispondrán de todas las facultades de supervisión, investigación y sanción necesarias para cumplir sus obligaciones con arreglo al presente Reglamento.

123. Las facultades a que se refiere el apartado 1 incluirán, como mínimo, las siguientes:

(rrrrrr) tener acceso a cualquier documento o a los datos bajo cualquier forma que la autoridad competente considere relevantes para el ejercicio de sus funciones y recibir o procurarse copia de los mismos;

(ssssss) realizar investigaciones o inspecciones *in situ*;

(tttttt) exigir medidas correctoras en caso de incumplimiento de los requisitos del presente Reglamento.

124. Sin perjuicio del derecho de los Estados miembros a imponer sanciones penales de conformidad con el artículo 46, los Estados miembros establecerán normas que prevean sanciones administrativas y medidas correctoras adecuadas en caso de incumplimiento del presente Reglamento y garantizarán su aplicación efectiva.

Dichas sanciones y medidas serán eficaces, proporcionadas y disuasorias.

125. Los Estados miembros conferirán a las autoridades competentes la facultad de aplicar al menos las siguientes sanciones administrativas o medidas correctoras en caso de incumplimiento del presente Reglamento:

(uuuuuu) formular un requerimiento dirigido a la persona física o jurídica para que ponga fin a su conducta y se abstenga de repetirla;

(vvvvvv) exigir el cese provisional o definitivo de toda práctica o conducta que la autoridad competente considere contraria a las disposiciones del presente Reglamento e impedir la repetición de dicha práctica o conducta;

(wwwwww) adoptar cualquier tipo de medida, incluso de carácter pecuniario, para garantizar que las entidades financieras sigan cumpliendo los requisitos legales;

(xxxxxx) exigir, en la medida en que lo permita la legislación nacional, los registros de tráfico de datos existentes que obren en poder de un operador de telecomunicaciones, cuando existan sospechas fundadas de infracción del

presente Reglamento y cuando tales registros puedan ser pertinentes para una investigación de infracciones del presente Reglamento, y

(yyyyyy) publicar avisos, incluidas declaraciones públicas en las que se indique la identidad de la persona física o jurídica y la naturaleza de la infracción.

126. Cuando las disposiciones a que se refieren el apartado 2, letra c), y el apartado 4 se apliquen a personas jurídicas, los Estados miembros conferirán a las autoridades competentes la facultad de aplicar las sanciones administrativas y las medidas correctoras, sin perjuicio de las condiciones que establezca el Derecho nacional, a los miembros del órgano de dirección y a las demás personas físicas que, conforme al Derecho nacional, sean responsables de la infracción.

127. Los Estados miembros velarán por que cualquier decisión de imponer sanciones administrativas o medidas correctoras conforme a lo establecido en el apartado 2, letra c), esté debidamente motivada y pueda ser objeto de recurso.

Artículo 45

Ejercicio de la facultad de imponer sanciones administrativas y medidas correctoras

128. Las autoridades competentes ejercerán las facultades de imponer las sanciones administrativas y las medidas correctoras a que se refiere el artículo 44 de conformidad con sus ordenamientos jurídicos nacionales, según proceda:

(zzzzzz) directamente;

(aaaaaaa) en colaboración con otras autoridades;

(bbbbbbb) bajo su responsabilidad, mediante delegación en otras autoridades;

(ccccccc) mediante solicitud dirigida a las autoridades judiciales competentes.

129. Al determinar el tipo y el nivel de una sanción administrativa o medida correctora impuesta de conformidad con el artículo 44, las autoridades competentes tendrán en cuenta si la infracción es intencionada o es consecuencia de una negligencia y cualesquiera otras circunstancias pertinentes, entre ellas, cuando proceda:

(ddddddd) la importancia, la gravedad y la duración de la infracción;

(eeeeeee) el grado de responsabilidad de la persona física o jurídica responsable de la infracción;

(fffffff) la solidez financiera de la persona física o jurídica responsable;

(ggggggg) la importancia de los beneficios obtenidos o las pérdidas evitadas por la persona física o jurídica responsable, en la medida en que puedan determinarse;

(hhhhhhh) las pérdidas causadas a terceros por la infracción, en la medida en que puedan determinarse;

(iiiiiii) el grado de cooperación de la persona física o jurídica responsable con la autoridad competente, sin perjuicio de la obligación de que dicha persona restituya las ganancias obtenidas o las pérdidas evitadas;

(jjjjjjj) las infracciones anteriores de la persona física o jurídica responsable.

Artículo 46

Sanciones penales aplicables

130. Los Estados miembros podrán decidir no establecer normas que prevean sanciones administrativas o medidas correctoras para las infracciones que estén sujetas a sanciones penales con arreglo a su Derecho nacional.

131. Los Estados miembros que opten por establecer sanciones penales por infracciones del presente Reglamento se asegurarán de que se hayan adoptado las medidas adecuadas para que las autoridades competentes dispongan de todas las facultades necesarias a fin de ponerse en contacto con las autoridades judiciales o las responsables de la fiscalía o de la justicia penal dentro de su jurisdicción, con el fin de obtener información específica relacionada con las investigaciones o procesos penales iniciados por infracciones del presente Reglamento, y de facilitar información del mismo tenor a otras autoridades competentes y a la ABE, la AEVM o la AESPJ, en cumplimiento de su obligación de cooperar a los efectos del presente Reglamento.

Artículo 47

Obligaciones de notificación

Los Estados miembros notificarán a la Comisión, a la AEVM, la ABE y la AESPJ las disposiciones legales, reglamentarias y administrativas de transposición del presente capítulo a más tardar el [*DO: insértese la fecha correspondiente a 1 año después de la fecha de entrada en vigor*]. Los Estados miembros notificarán sin demora indebida cualquier modificación ulterior de dichas disposiciones a la Comisión, la AEVM, la ABE y la AESPJ.

Artículo 48

Publicación de las sanciones administrativas

132. Las autoridades competentes publicarán en sus sitios web oficiales, sin demora indebida, toda decisión por la que se imponga una sanción administrativa contra la que no haya lugar a recurso tras la notificación de dicha decisión al destinatario de la sanción.

133. La publicación a que se refiere el apartado 1 incluirá información sobre el tipo y la naturaleza de la infracción, la identidad de las personas responsables y las sanciones impuestas.

134. Cuando la autoridad competente, tras una evaluación de cada caso, considere que la publicación de la identidad, cuando se trate de personas jurídicas, o de la identidad y los datos personales, cuando se trate de personas físicas, sería desproporcionada, pondría en peligro la estabilidad de los mercados financieros o la continuación de una investigación penal en curso, o causaría a la persona afectada daños desproporcionados, en la medida en que estos puedan determinarse, adoptará una de las siguientes soluciones con respecto a la decisión por la que se imponga una sanción administrativa:

(kkkkkkk) aplazar su publicación hasta el momento en que dejen de existir todos los motivos para no publicarla;

(lllllll) publicarla de forma anónima, de conformidad con la legislación nacional; o

(mmmmmmm) abstenerse de publicarla, si las opciones enunciadas en las letras a) y b) se consideran insuficientes para garantizar que la estabilidad de los mercados financieros no corra peligro, o cuando dicha publicación no sea proporcionada a la indulgencia de la sanción impuesta.

135. En caso de que se decida publicar una sanción administrativa de forma anónima como se establece en el apartado 3, letra b), podrá aplazarse la publicación de los datos pertinentes.

136. Cuando una autoridad competente publique una decisión que imponga una sanción administrativa que pueda recurrirse ante las autoridades judiciales pertinentes, las autoridades competentes añadirán de forma inmediata en su sitio web oficial dicha información y, con posterioridad, cualquier información ulterior relacionada sobre el resultado del recurso. Cualquier resolución judicial que anule una decisión que imponga una sanción administrativa también deberá publicarse.

137. Las autoridades competentes garantizarán que toda publicación a que se hace referencia en los apartados 1 a 4 permanezca en su sitio web oficial durante al menos cinco años tras su publicación. Los datos personales que figuren en la publicación solo se mantendrán en el sitio web oficial de la autoridad competente durante el tiempo que resulte necesario de acuerdo con las normas aplicables en materia de protección de datos.

Artículo 49

Secreto profesional

138. Toda información confidencial recibida, intercambiada o transmitida en virtud del presente Reglamento estará sujeta a las condiciones de secreto profesional establecidas en el apartado 2.

139. La obligación de secreto profesional se aplicará a todas las personas que trabajen o hayan trabajado para las autoridades competentes en virtud del presente Reglamento o para cualquier otra autoridad u organismo del mercado o persona física o jurídica en los que aquellas hayan delegado sus facultades, incluidos los auditores y expertos contratados por ellas.

140. La información sujeta al secreto profesional no podrá divulgarse a ninguna otra persona o autoridad, salvo en virtud del Derecho de la Unión o nacional.

141. Toda la información intercambiada por las autoridades competentes en virtud del presente Reglamento y referida a las condiciones comerciales u operativas, así como a otros asuntos de tipo económico o personal, se considerará confidencial y estará amparada por el secreto profesional, salvo cuando la autoridad competente declare, en el momento de su comunicación, que la información puede ser revelada o esta revelación resulte necesaria en el marco de un procedimiento judicial.

CAPÍTULO VIII

ACTOS DELEGADOS

Artículo 50

Ejercicio de la delegación

142. Los poderes para adoptar actos delegados se otorgan a la Comisión en las condiciones que se establecen en el presente artículo.

143. Los poderes para adoptar los actos delegados a que se refieren el artículo 28, apartado 3, y el artículo 38, apartado 2, se otorgan a la Comisión por un período de cinco años a partir del [*OP: insértese la fecha correspondiente a 5 años después de la fecha de entrada en vigor*].

144. La delegación de poderes mencionada en el artículo 28, apartado 3, y en el artículo 38, apartado 2, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. Surtirá efecto el día siguiente al de su publicación en el *Diario Oficial de la Unión Europea* o en una fecha posterior indicada en la misma. No afectará a la validez de los actos delegados que ya estén en vigor.

145. Antes de la adopción de un acto delegado, la Comisión consultará a los expertos designados por cada Estado miembro de conformidad con los principios establecidos en el Acuerdo interinstitucional sobre la mejora de la legislación de 13 de abril de 2016.

146. En cuanto la Comisión adopte un acto delegado lo notificará simultáneamente al Parlamento Europeo y al Consejo.

147. Los actos delegados adoptados de conformidad con el artículo 28, apartado 3, y con el artículo 38, apartado 2, entrarán en vigor únicamente si, en un plazo de dos meses a partir de su notificación al Parlamento Europeo y al Consejo, ninguna de estas instituciones formula objeciones o si, antes del vencimiento de dicho plazo, ambas informan a la Comisión de que no las formularán. El plazo se prorrogará dos meses a iniciativa del Parlamento Europeo o del Consejo.

CAPÍTULO IX

DISPOSICIONES TRANSITORIAS Y FINALES

SECCIÓN I

Artículo 51

Cláusula de revisión

A más tardar el [*OP: insértese la fecha correspondiente a 5 años después de la fecha de entrada en vigor*], la Comisión, previa consulta a la ABE, la AEVM, la AESPJ y la JERS, según proceda, llevará a cabo una revisión y presentará al Parlamento Europeo y al Consejo un informe, acompañado, si procede, de una propuesta legislativa, sobre los criterios para la

designación de proveedores terceros esenciales de servicios de TIC contemplados en el artículo 28, apartado 2.

SECCIÓN II

MODIFICACIONES

Artículo 52

Modificaciones del Reglamento (CE) n.º 1060/2009

En el anexo I, sección A, punto 4, del Reglamento (CE) n.º 1060/2009, el párrafo primero se sustituye por el texto siguiente:

«Las agencias de calificación crediticia dispondrán de procedimientos administrativos y contables adecuados, mecanismos de control interno, técnicas eficaces de valoración del riesgo y mecanismos eficaces de control y salvaguardia para gestionar sus sistemas de TIC de conformidad con el Reglamento (UE) 2021/xx del Parlamento Europeo y del Consejo* [DORA].

* Reglamento (UE) 2021/xx del Parlamento Europeo y del Consejo […] (DO L XX, D.M.AAAA, p. X).».

Artículo 53

Modificaciones del Reglamento (UE) n.º 648/2012

El Reglamento (UE) n.º 648/2012 se modifica como sigue:

(51) El artículo 26 se modifica como sigue:

(a) el apartado 3 se sustituye por el texto siguiente:

«3. Las ECC mantendrán y aplicarán una estructura organizativa que garantice la continuidad y el correcto funcionamiento de la prestación de sus servicios y la realización de sus actividades. Empleará sistemas, recursos y procedimientos adecuados y proporcionados, incluidos sistemas de TIC gestionados de conformidad con el Reglamento (UE) 2021/xx del Parlamento Europeo y del Consejo* [DORA].

* Reglamento (UE) 2021/xx del Parlamento Europeo y del Consejo […] (DO L XX, D.M.AAAA, p. X).».

(b) se suprime el apartado 6.

(52) El artículo 34 se modifica como sigue:

(a) el apartado 1 se sustituye por el texto siguiente:

«1. Las ECC establecerán, aplicarán y mantendrán una estrategia adecuada de continuidad de la actividad y de recuperación en caso de catástrofe, que incluirá planes de continuidad de la actividad y de recuperación en caso de catástrofe relacionados con las TIC establecidos de conformidad con el Reglamento (UE) 2021/xx [DORA], destinada a garantizar la preservación de sus funciones, la oportuna recuperación de las operaciones y el cumplimiento de sus obligaciones.»;

(b) en el apartado 3, el párrafo primero se sustituye por el texto siguiente:

«A fin de asegurar la aplicación coherente del presente artículo, la AEVM, previa consulta a los miembros del SEBC, elaborará proyectos de normas técnicas reglamentarias en las que se especifiquen el contenido y los requisitos mínimos de la política de continuidad de la actividad y del plan de recuperación en caso de catástrofe, excluidos los planes de continuidad de la actividad y recuperación en caso de catástrofe relacionados con las TIC.».

(53) En el artículo 56, apartado 3, el párrafo primero se sustituye por el texto siguiente:

«3. A fin de asegurar la aplicación coherente del presente artículo, la AEVM elaborará proyectos de normas técnicas de regulación en las que se especifiquen los pormenores, que no sean los relativos a los requisitos relacionados con la gestión del riesgo de TIC, de la solicitud de inscripción a que se refiere el apartado 1.».

(54) En el artículo 79, los apartados 1 y 2 se sustituyen por el texto siguiente:

«1. Los registros de operaciones determinarán las fuentes de riesgo operativo y las reducirán al mínimo también mediante el desarrollo de sistemas, controles y procedimientos adecuados, incluidos sistemas de TIC gestionados de conformidad con el Reglamento (UE) 2021/xx [DORA].

2. Los registros de operaciones establecerán, aplicarán y mantendrán una estrategia adecuada de continuidad de la actividad y de recuperación en caso de catástrofe, que incluirá planes de continuidad de la actividad y de recuperación en caso de catástrofe relacionados con las TIC establecidos de conformidad con el Reglamento (UE) 2021/xx [DORA], destinada a garantizar el mantenimiento de sus funciones, la oportuna recuperación de las operaciones y el cumplimiento de sus obligaciones.».

(55) En el artículo 80, se suprime el apartado 1.

Artículo 54

Modificaciones del Reglamento (UE) n.º 909/2014

El artículo 45 del Reglamento (UE) n.º 909/2014 se modifica como sigue:

(56) el apartado 1 se sustituye por el texto siguiente:

«1. Los DCV determinarán las fuentes de riesgo operativo, tanto internas como externas, y minimizarán su impacto también mediante la implantación de las herramientas, procesos y políticas de TIC adecuados establecidos y gestionados de conformidad con el Reglamento (UE) 2021/xx del Parlamento Europeo y del Consejo* [DORA], así como mediante cualesquiera otros instrumentos, controles y procedimientos pertinentes para otros tipos de riesgo operativo, en relación con todos los sistemas de liquidación de valores que operen.

* Reglamento (UE) 2021/xx del Parlamento Europeo y del Consejo […] (DO L XX, DD.MM.YYYY, p. X).».

(57) se suprime el apartado 2;

(58) los apartados 3 y 4 se sustituyen por el texto siguiente:

«3. En lo que respecta a los servicios que presten, y en relación con cada sistema de liquidación de valores que exploten, los DCV definirán, implantarán y mantendrán un plan adecuado de continuidad de la actividad y recuperación en caso de catástrofe, incluidos planes de continuidad de la actividad y recuperación en caso de catástrofe relacionados con las TIC establecidos de conformidad con el Reglamento (UE) 2021/xx [DORA], a fin de garantizar el mantenimiento de sus servicios, la oportuna recuperación de las operaciones y el cumplimiento de las obligaciones del DCV ante acontecimientos que supongan un riesgo significativo de perturbación de las operaciones.

4. El plan a que se refiere el apartado 3 deberá prever la recuperación de todas las operaciones y posiciones de los participantes en el momento de la perturbación, con objeto de que los participantes del DCV puedan seguir operando con certeza y finalizar la liquidación en la fecha programada, para lo cual el plan deberá garantizar, en particular, que los sistemas informáticos esenciales puedan reanudar las operaciones tras la perturbación, según lo establecido en el artículo 11, apartados 5 y 7, del Reglamento (UE) 2021/xx [DORA].»;

(59) en el apartado 6, el párrafo primero se sustituye por el texto siguiente:

«Los DCV determinarán, controlarán y gestionarán los riesgos que los participantes más importantes de los sistemas de liquidación de valores que gestionan, así como los prestadores de servicios y otros DCV u otras infraestructuras del mercado pueden suponer para su funcionamiento. Facilitarán a las autoridades competentes y relevantes, a petición de estas, información sobre todo riesgo de este tipo que se detecte. Informarán asimismo sin dilación a las autoridades competentes y las autoridades relevantes de todo incidente operativo, que no esté relacionado con el riesgo de TIC, resultante de tales riesgos.»;

(60) en el apartado 7, el párrafo primero se sustituye por el texto siguiente:

«La AEVM, en estrecha cooperación con los miembros del SEBC, elaborará proyectos de normas técnicas de regulación que especifiquen los riesgos operativos a que se refieren los apartados 1 y 6, que no sean riesgos de TIC, los métodos para probar, afrontar o minimizar tales riesgos, en particular los planes de continuidad de la actividad y de recuperación en caso de catástrofe a que se refieren los apartados 3 y 4, y los correspondientes métodos de evaluación.».

Artículo 55

Modificaciones del Reglamento (UE) n.º 600/2014

El Reglamento (UE) n.º 600/2014 se modifica como sigue:

(61) El artículo 27 *octies* se modifica como sigue:

(a) se suprime el apartado 4;

(b) en el apartado 8, la letra c) se sustituye por el texto siguiente:

(c) «c) los requisitos concretos de organización establecidos en los apartados 3 y 5.».

(62) El artículo 27 *nonies* se modifica como sigue:

(a) se suprime el apartado 5;

(b) en el apartado 8, la letra e) se sustituye por el texto siguiente:

«e) los requisitos concretos de organización establecidos en el apartado 4.».

(63) El artículo 27 *decies* se modifica como sigue:

(a) se suprime el apartado 3;

(b) en el apartado 5, la letra b) se sustituye por el texto siguiente:

«b) los requisitos concretos de organización establecidos en los apartados 2 y 4.».

Artículo 56

Entrada en vigor y aplicación

El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

Será aplicable a partir del [*OP: insértese la fecha correspondiente a 12 meses después de la fecha de entrada en vigor*].

No obstante, los artículos 23 y 24 serán de aplicación a partir del [*OP: insértese la fecha correspondiente a 36 meses después de la fecha de entrada en vigor*].

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el

Por el Parlamento Europeo	*Por el Consejo*
El Presidente / La Presidenta	*El Presidente / La Presidenta*

FICHA FINANCIERA LEGISLATIVA

1. MARCO DE LA PROPUESTA/INICIATIVA

1.1. Denominación de la propuesta/iniciativa

1.2. Política(s) afectada(s)

1.3. Naturaleza de la propuesta/iniciativa

1.4. Objetivo(s)

1.5. Justificación de la propuesta/iniciativa

1.6. Duración e incidencia financiera de la propuesta/iniciativa

1.7. Modo(s) de gestión previsto(s)

2. MEDIDAS DE GESTIÓN

2.1. Disposiciones en materia de seguimiento e informes

2.2. Sistema(s) de gestión y de control

2.3. Medidas de prevención del fraude y de las irregularidades

3. INCIDENCIA FINANCIERA ESTIMADA DE LA PROPUESTA/INICIATIVA

3.1. Rúbrica(s) del marco financiero plurianual y línea(s) presupuestaria(s) de gastos afectada(s)

3.2. Incidencia estimada en los gastos

3.2.1. Resumen de la incidencia estimada en los gastos

3.2.2. Incidencia estimada en los créditos

3.2.3. Incidencia estimada en los recursos humanos

3.2.4. Compatibilidad con el marco financiero plurianual vigente

3.2.5. Contribución de terceros

3.3. Incidencia estimada en los ingresos

Anexo

Supuestos generales

Facultades de supervisión

FICHA FINANCIERA LEGISLATIVA «AGENCIAS»

148. MARCO DE LA PROPUESTA/INICIATIVA

148.1. Denominación de la propuesta/iniciativa

Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre la resiliencia operativa digital del sector financiero.

148.2. Política(s) afectada(s)

Ámbito de actuación: Estabilidad financiera, servicios financieros y Unión de los Mercados de Capitales

Actividad: Resiliencia operativa digital

148.3. La propuesta se refiere a

☑ **una acción nueva**

☐ **una acción nueva a raíz de un proyecto piloto / una acción preparatoria**[50]

☐ **la prolongación de una acción existente**

☐ **una fusión o reorientación de una o más acciones hacia otra/una nueva acción**

148.4. Objetivo(s)

148.4.1. Objetivo(s) general(es)

El objetivo general de la iniciativa es reforzar la resiliencia operativa digital de las entidades del sector financiero de la UE simplificando y modernizando las normas existentes e introduciendo nuevos requisitos allí donde existen lagunas. Esto mejoraría también el código normativo único en su dimensión digital.

El objetivo global puede estructurarse en tres objetivos generales: 1) reducir el riesgo de perturbación e inestabilidad financieras, 2) reducir la carga administrativa y aumentar la eficacia de la supervisión, y 3) aumentar la protección de los consumidores y los inversores.

148.4.2. Objetivo(s) específico(s)

La propuesta persigue los objetivos específicos siguientes:

Hacer frente a los riesgos de las tecnologías de la información y la comunicación (TIC) de forma más exhaustiva y reforzar el nivel global de resiliencia digital del sector financiero.

Simplificar la notificación de incidentes relacionados con las TIC y corregir la duplicación de requisitos de notificación.

Permitir el acceso de los supervisores financieros a la información sobre incidentes relacionados con las TIC.

[50] Tal como se contempla en el artículo 58, apartado 2, letras a) o b), del Reglamento Financiero..

Garantizar que las entidades financieras reguladas por la presente propuesta evalúen la eficacia de sus medidas preventivas y de resiliencia y detecten las vulnerabilidades relacionadas con las TIC. Reducir la fragmentación del mercado único y hacer posible la aceptación transfronteriza de los resultados de las pruebas. Reforzar las salvaguardias contractuales que amparan a las entidades financieras cuando utilizan servicios de TIC, incluidas las normas de externalización (que rigen el seguimiento de los proveedores terceros de TIC). Permitir una supervisión de las actividades de los proveedores terceros esenciales de TIC. Incentivar el intercambio de inteligencia sobre amenazas en el sector financiero.

148.4.3. Resultado(s) e incidencia esperados

Especifíquense los efectos que la propuesta/iniciativa debería tener sobre los beneficiarios / la población destinataria.

Un acto sobre resiliencia operativa digital para el sector financiero garantizaría un marco global que abarcaría todos los aspectos de la resiliencia operativa digital y sería eficaz para mejorar la resiliencia operativa general del sector financiero. Preservaría la claridad y la coherencia en el código normativo único.

También haría más clara y coherente la interacción con la Directiva sobre seguridad de las redes y de la información y su revisión. Aportaría a las entidades financieras claridad sobre las diferentes normas de resiliencia operativa digital que deben cumplir, en particular a las entidades financieras que poseen varias autorizaciones y operan en diferentes mercados dentro de la UE.

148.4.4. Indicadores de rendimiento

Especifíquense los indicadores que permitan hacer un seguimiento de los avances y logros.

Indicadores posibles:

Número de incidentes relacionados con las TIC en el sector financiero de la UE y su repercusión

Número de incidentes graves relacionados con las TIC notificados a los supervisores prudenciales

Número de entidades financieras que deberían llevar a cabo pruebas de penetración guiadas por amenazas

Número de entidades financieras que utilizan cláusulas contractuales estándar para celebrar acuerdos contractuales con proveedores terceros de servicios de TIC

Número de proveedores terceros esenciales de TIC supervisados por las AES / los supervisores prudenciales

Número de entidades financieras que participan en soluciones de intercambio de inteligencia sobre amenazas

Número de autoridades que recibirán informes sobre el mismo incidente relacionado con las TIC

Número de pruebas transfronterizas de penetración guiadas por amenazas

148.5. Justificación de la propuesta/iniciativa

148.5.1. Necesidad(es) que debe(n) satisfacerse a corto o largo plazo, incluido un calendario detallado de la aplicación de la iniciativa

El sector financiero hace un extenso uso de las tecnologías de la información y la comunicación (TIC). Pese a los significativos avances realizados a través de iniciativas estratégicas y legislativas específicas a nivel nacional y europeo, los riesgos de TIC siguen planteando un reto para la resiliencia operativa, el funcionamiento y la estabilidad del sistema financiero de la UE. La reforma que siguió a la crisis financiera de 2008 reforzó fundamentalmente la resiliencia financiera del sector financiero de la UE y tuvo por objeto salvaguardar la competitividad y la estabilidad de la UE frente a las perspectivas económicas, prudenciales y de conducta del mercado. La seguridad de las TIC y, en términos generales, la resiliencia operativa digital forman parte del riesgo operativo, pero han recibido menos

atención en el programa regulador posterior a la crisis, y se han desarrollado solo en algunos ámbitos de las políticas y la regulación de los mercados financieros de la UE, o solo en determinados Estados miembros. Esto ocasiona los siguientes problemas, que la propuesta debe resolver:

El marco jurídico de la UE que regula el riesgo de TIC y la resiliencia operativa en el sector financiero en su conjunto está fragmentado y no es completamente coherente.

La falta de coherencia de los requisitos de notificación de los incidentes relacionados con las TIC hace que los supervisores tengan una visión incompleta de la naturaleza, la frecuencia, la importancia y la repercusión de dichos incidentes.

Algunas entidades financieras están sujetas a requisitos de notificación complejos, duplicados y potencialmente incoherentes en relación con el mismo incidente relacionado con las TIC.

Un nivel insuficiente de intercambio de información y cooperación en materia de inteligencia sobre ciberamenazas a nivel estratégico, táctico y operativo impide que las distintas entidades financieras evalúen y supervisen cabalmente las ciberamenazas y que opongan a ellas una defensa y una respuesta adecuadas.

En algunos subsectores financieros, puede haber marcos de pruebas de penetración y resiliencia múltiples y descoordinados, a lo que acompaña la falta de reconocimiento transfronterizo de los resultados, mientras que otros subsectores carecen de tales marcos de prueba.

La falta de conocimientos a efectos de supervisión sobre las actividades de las entidades financieras que recurren a los servicios de proveedores terceros de TIC expone a las entidades financieras individualmente, y al sistema financiero en su conjunto, a riesgos operativos.

Los supervisores financieros no disponen de un mandato suficiente ni de herramientas para supervisar y gestionar los riesgos de concentración y sistémicos que se derivan de la dependencia de las entidades financieras respecto de proveedores terceros de TIC.

148.5.2. Valor añadido de la intervención de la Unión (puede derivarse de distintos factores, como mejor coordinación, seguridad jurídica, mejora de la eficacia o complementariedades). A efectos del presente punto, se entenderá por «valor añadido de la intervención de la Unión» el valor resultante de una intervención de la Unión que viene a sumarse al valor que se habría generado de haber actuado los Estados miembros de forma aislada.

Motivos para actuar a nivel europeo (*ex ante*):

La resiliencia operativa digital es una cuestión de interés común para los mercados financieros de la UE. La actuación a nivel de la UE aportaría más ventajas y valor que la adopción de medidas por separado a nivel nacional. Sin añadir estas disposiciones operativas sobre el riesgo de TIC, el código normativo único proporcionaría las herramientas para hacer frente a todos los demás tipos de riesgo a escala europea, pero pasaría por alto los aspectos relativos a la resiliencia operativa digital o los sometería a iniciativas a nivel nacional fragmentadas y descoordinadas. La propuesta aportaría claridad jurídica acerca de si se aplican las disposiciones sobre operatividad digital y de qué manera, especialmente para las entidades financieras transfronterizas, y haría innecesario que los Estados miembros mejorasen individualmente las normas, los estándares y las expectativas en relación con la resiliencia operativa y la ciberseguridad como respuesta a la actual cobertura limitada de las normas de la UE y a las características generales de la Directiva sobre seguridad de las redes y de la información.

Valor añadido de la Unión que se prevé generar (*ex post*): La intervención de la Unión aumentaría significativamente la eficacia de la política, al mismo tiempo que reduciría la complejidad y aliviaría la carga financiera y administrativa de todas las entidades financieras. Armonizaría un ámbito de la economía que está muy profundamente interconectado e integrado y que ya se beneficia de un conjunto único de normas y supervisión. Por lo que respecta a la notificación de incidentes relacionados con las TIC, la propuesta reduciría la carga que supondría tener que notificar el mismo incidente relacionado con las TIC a diferentes autoridades de la UE y/o nacionales, así como los costes consiguientes. Además, facilitará el reconocimiento y la aceptación mutuos de los resultados de las pruebas de las entidades que operan a escala transfronteriza y que están sujetas a múltiples marcos de pruebas en diferentes Estados miembros.

148.5.3. Principales conclusiones extraídas de experiencias similares anteriores

Nueva iniciativa

148.5.4. Compatibilidad con el marco financiero plurianual y posibles sinergias con otros instrumentos adecuados

El objetivo de la presente propuesta es coherente con otras políticas e iniciativas en curso de la UE, en particular la Directiva sobre seguridad de las redes y de la información (SRI) y la Directiva sobre infraestructuras críticas europeas (ICE). La propuesta preservaría los beneficios asociados al marco horizontal en materia de ciberseguridad, al mantener los tres subsectores financieros dentro del ámbito de aplicación de la Directiva sobre seguridad de las redes y de la información. Al seguir asociados al ecosistema de esta Directiva, los supervisores financieros podrían intercambiar información pertinente con las autoridades de SRI y participar en el Grupo de cooperación sobre SRI. La propuesta no afectaría a la Directiva SRI, sino que se basaría en ella y en caso de solapamiento aplicaría el principio de *lex specialis*. La interacción entre la regulación de los servicios financieros y la Directiva SRI seguiría rigiéndose por una cláusula de *lex specialis*, lo que eximiría a las entidades financieras de cumplir los requisitos sustantivos de la Directiva SRI y evitaría solapamientos entre ambos actos. Además, la propuesta es coherente con la Directiva sobre infraestructuras críticas europeas (ICE), actualmente en proceso de revisión para mejorar la protección y la resiliencia de las infraestructuras críticas frente a las amenazas no cibernéticas.

La presente propuesta no tendría incidencia en el marco financiero plurianual (MFP). En primer lugar, el marco de supervisión de los proveedores terceros esenciales de TIC se financiará íntegramente mediante las tasas cobradas a estos proveedores; en segundo lugar, las tareas reguladoras adicionales relacionadas con la resiliencia operativa digital encomendadas a las AES se llevarán a cabo mediante la redistribución interna del personal existente.

Esto se traducirá en una propuesta para aumentar el personal autorizado de la agencia durante el futuro procedimiento presupuestario anual. La agencia continuará trabajando para maximizar las sinergias y la eficiencia (entre otras cosas, a través de los sistemas informáticos) y seguirá de cerca el aumento de la carga de trabajo asociado a esta propuesta, que se reflejaría en el nivel de personal autorizado solicitado por la agencia en el procedimiento presupuestario anual.

148.5.5. Evaluación de las diferentes opciones de financiación disponibles, incluidas las posibilidades de reasignación

Se consideraron varias opciones de financiación:

En primer lugar, los costes adicionales podrían financiarse a través del mecanismo de financiación habitual de las AES. Sin embargo, esto implicaría un aumento sustancial de la contribución de la UE a los recursos financieros de las AES.

Esta es la opción elegida para los costes relacionados con las tareas reguladoras vinculadas a la presente propuesta. Así, se pedirá a las AES que redistribuyan el personal existente para elaborar una serie de normas técnicas. Sin embargo, los costes adicionales relacionados con la supervisión de los proveedores terceros esenciales no podrían cubrirse mediante una redistribución de recursos dentro de las AES, que, además de las previstas en la presente propuesta, desempeñan también otras tareas en virtud de otros actos legislativos de la Unión. Además, las tareas de supervisión relacionadas con la resiliencia operativa digital requieren conocimientos técnicos y experiencia específicos. Puesto que el nivel actual de esos recursos en las AES es insuficiente, se necesitan recursos adicionales.

Por último, de acuerdo con la propuesta, se cobrarán tasas a los proveedores terceros esenciales de TIC sujetos a supervisión. Con ellas se pretende sufragar todos los recursos adicionales que necesitarán las AES para ejercer sus nuevas funciones y facultades.

148.6. Duración e incidencia financiera de la propuesta/iniciativa

☐ **duración limitada**

☐ Propuesta/iniciativa en vigor desde [el] [DD.MM.]AAAA hasta [el] [DD.MM.]AAAA

☐ Incidencia financiera desde AAAA hasta AAAA

☑ **duración ilimitada**

Ejecución con una fase de puesta en marcha a partir de 2021,

y pleno funcionamiento a partir de la última fecha.

148.7. Modo(s) de gestión previsto(s) [51]

Gestión directa a cargo de la Comisión

☐ por las agencias ejecutivas

☐ **Gestión compartida** con los Estados miembros

☑ **Gestión indirecta** mediante delegación de tareas de ejecución presupuestaria en:

☐ organizaciones internacionales y sus agencias (especifíquense);

☐ el BEI y el Fondo Europeo de Inversiones;

☑ los organismos contemplados en los artículos 70 y 71;

☐ organismos de Derecho público;

☐ organismos de Derecho privado investidos de una misión de servicio público, en la medida en que presenten garantías financieras suficientes;

☐ organismos de Derecho privado de un Estado miembro a los que se haya encomendado la ejecución de una colaboración público-privada y que presenten garantías financieras suficientes;

☐ personas a quienes se haya encomendado la ejecución de acciones específicas en el marco de la PESC, de conformidad con el título V del Tratado de la Unión Europea, y que estén identificadas en el acto de base correspondiente.

Observaciones

N. a.

[51] Las explicaciones sobre los modos de gestión y las referencias al Reglamento Financiero pueden consultarse en el sitio BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

149. MEDIDAS DE GESTIÓN

149.1. Disposiciones en materia de seguimiento e informes

Especifíquense la frecuencia y las condiciones de dichas disposiciones.

De acuerdo con disposiciones ya en vigor, las AES preparan regularmente informes sobre su actividad (incluidos informes internos a la alta dirección, informes a las Juntas y un informe anual) y la utilización de sus recursos y su rendimiento son objeto de auditorías del Tribunal de Cuentas y del servicio de auditoría interna de la Comisión. El seguimiento de las acciones incluidas en la propuesta y los informes correspondientes se ajustarán a los requisitos ya existentes, así como a los nuevos requisitos derivados de la presente propuesta.

149.2. Sistema(s) de gestión y de control

149.2.1. Justificación del modo o los modos de gestión, el mecanismo o los mecanismos de ejecución de la financiación, las modalidades de pago y la estrategia de control propuestos

La gestión será indirecta a través de las AES. El mecanismo de financiación se implementaría a través de tasas cobradas a los proveedores terceros esenciales de TIC de que se trate.

149.2.2. Información relativa a los riesgos detectados y al sistema o los sistemas de control interno establecidos para mitigarlos

En cuanto a un uso legal, económico, eficiente y eficaz de los créditos que se deriven de la propuesta, se prevé que esta no generará nuevos riesgos significativos que no estén cubiertos por un marco de control interno vigente. Sin embargo, una nueva dificultad podría estar relacionada con el cobro puntual de las tasas a los proveedores terceros esenciales de TIC de que se trate.

149.2.3. Estimación y justificación de la relación coste/beneficio de los controles (ratio «gastos de control ÷ valor de los correspondientes fondos gestionados»), y evaluación del nivel esperado de riesgo de error (al pago y al cierre)

Los sistemas de gestión y control establecidos en los Reglamentos de las AES ya se aplican. Las AES cooperan estrechamente con el servicio de auditoría interna de la Comisión a fin de velar por el cumplimiento de las normas pertinentes en todos los ámbitos del marco de control interno. Estas disposiciones se aplicarán también a la función de las AES prevista en la presente propuesta. Además, en cada ejercicio, el Parlamento Europeo, previa recomendación del Consejo, aprueba la gestión de cada AES en la ejecución de su presupuesto.

149.3. Medidas de prevención del fraude y de las irregularidades

Especifíquense las medidas de prevención y protección existentes o previstas, por ejemplo, en la estrategia de lucha contra el fraude.

A efectos de la lucha contra el fraude, la corrupción y cualesquiera otras prácticas contrarias a Derecho, se aplicarán a las AES sin restricciones las disposiciones del Reglamento (UE, Euratom) n.º 883/2013 del Parlamento Europeo y del Consejo, de 11 de septiembre de 2013, relativo a las investigaciones efectuadas por la Oficina Europea de Lucha contra el Fraude (OLAF).

Las AES tienen una estrategia específica de lucha contra el fraude y el consiguiente plan de acción. Las medidas reforzadas de las AES en el ámbito de la lucha contra el fraude se ajustarán a las normas y orientaciones proporcionadas por el Reglamento Financiero (medidas de lucha contra el fraude en el marco de una buena gestión financiera), las políticas de prevención del fraude de la OLAF, las disposiciones previstas por la estrategia de la Comisión de lucha contra el fraude [COM(2011) 376], así como las establecidas en el enfoque común sobre las agencias descentralizadas de la UE (julio de 2012) y el correspondiente plan de trabajo.

Por otra parte, los Reglamentos por los que se crean las AES y los Reglamentos financieros de las AES establecen las disposiciones relativas a la ejecución y el control de sus presupuestos y las normas financieras aplicables, incluidas las destinadas a prevenir el fraude y las irregularidades.

150. INCIDENCIA FINANCIERA ESTIMADA DE LA PROPUESTA/INICIATIVA

150.1. Rúbrica(s) del marco financiero plurianual y línea(s) presupuestaria(s) de gastos afectada(s)

Líneas presupuestarias existentes

En el orden de las rúbricas del marco financiero plurianual y las líneas presupuestarias.

Rúbrica del marco financiero plurianual	Línea presupuestaria	Tipo de gasto	Contribución			
	Número	CD/CND[52]	de países de la AELC[53]	de países candidatos[54]	de terceros países	a efectos de lo dispuesto en el artículo 21, apartado 2, letra b), del Reglamento Financiero

Nuevas líneas presupuestarias solicitadas

En el orden de las rúbricas del marco financiero plurianual y las líneas presupuestarias.

Rúbrica del marco financiero plurianual	Línea presupuestaria	Tipo de gasto	Contribución			
	Número	CD/CND	de países de la	de países	de terceros	a efectos de lo dispuesto en el

[52] CD = créditos disociados / CND = créditos no disociados s.

[53] AELC: Asociación Europea de Libre Comercio.

[54] Países candidatos y, en su caso, candidatos potenciales de los Balcanes Occidentales..

			AELC	candidatos	países	artículo 21, apartado 2, letra b), del Reglamento Financiero

150.2. Incidencia estimada en los gastos

150.3. Resumen de la incidencia estimada en los gastos

En millones EUR (al tercer decimal)

Rúbrica del marco financiero plurianual	Número	Rúbrica

DG: <..>			2020	2021	2022	2023	2024	2025	2026	2027	**TOTAL**
	Compromisos	(1)									
	Pagos	(2)									
TOTAL de los créditos para la DG <>	Compromisos										
	Pagos										

Rúbrica del marco financiero plurianual		

En millones EUR (al tercer decimal)

		2022	2023	2024	2025	2026	2027	**TOTAL**
DG:								
• Recursos humanos								
• Otros gastos administrativos <>								
TOTAL para las DG	Créditos							

TOTAL de los créditos para la RÚBRICA del marco financiero plurianual	(Total de los compromisos = total de los pagos)							

En millones EUR (al tercer decimal) a precios constantes

		2022	**2023**	**2024**	**2025**	**2026**	**2027**	**TOTAL**
TOTAL de los créditos para la RÚBRICA 1 del marco financiero plurianual	Compromisos							
	Pagos							

150.3.1. Incidencia estimada en los créditos

☑ La propuesta/iniciativa no exige la utilización de créditos de operaciones.

☐ La propuesta/iniciativa exige la utilización de créditos de operaciones, tal como se explica a continuación:

Créditos de compromiso en millones EUR (al tercer decimal) a precios constantes

Indíquense los objetivos y los resultados ⇩			2022		2023		2024		2025		2026		2027		**TOTAL**	
	RESULTADOS															
	Tipo[55]	Coste medio	Número	Coste	Número	Coste	Número	Coste	Número	Coste	Número	Coste	Número	Coste	Número total	Coste total
OBJETIVO ESPECÍFICO N.° 1[56] …																
- Resultado																
Subtotal del objetivo específico n.º 1																
OBJETIVO ESPECÍFICO N.° 2																
- Resultado																
Subtotal del objetivo específico n.º 2																
COSTE TOTAL																

[55] Los resultados son los productos y los servicios que se van a suministrar (por ejemplo: número de intercambios de estudiantes financiados, número de kilómetros de carretera construidos, etc.).

[56] Según lo descrito en el punto 1.4.2. «Objetivo(s) específico(s)…».

150.3.2. Incidencia estimada en los recursos humanos

150.3.2.1. Resumen

☐ La propuesta/iniciativa no exige la utilización de créditos administrativos.

☑ La propuesta/iniciativa exige la utilización de créditos administrativos, tal como se explica a continuación:

En millones EUR (al tercer decimal) a precios constantes

ABE, AESPJ, AEVM	2022	2023	2024	2025	2026	2027	**TOTAL**
Agentes temporales (Categoría AD)	1,188	2,381	2,381	2,381	2,381	2,381	13,093
Agentes temporales (Categoría AST)	0,238	0,476	0,476	0,476	0,476	0,476	2,618
Agentes contractuales							
Expertos nacionales en comisión de servicios							
TOTAL	1,426	2,857	2,857	2,857	2,857	2,857	15,711

Requisitos de personal (EJC):

ABE, AESPJ y AEVM	2022	2023	2024	2025	2026	2027	**TOTAL**
Agentes temporales (Categoría AD) ABE=5, AESPJ=5, AEVM=5	15	15	15	15	15	15	15
Agentes temporales (Categoría AST) ABE=1, AESPJ=1, AEVM=1	3	3	3	3	3	3	3
Agentes contractuales							
Expertos nacionales en comisión de servicios							
TOTAL	**18**	**18**	**18**	**18**	**18**	**18**	**18**

150.3.2.2. Necesidades estimadas de recursos humanos para las DG (matrices)

☑ La propuesta/iniciativa no exige la utilización de recursos humanos.

☐ La propuesta/iniciativa exige la utilización de recursos humanos, tal como se explica a continuación:

Estimación que debe expresarse en valores enteros (o, a lo sumo, con un decimal)

		2022	2023	2024	2025	2026	2027
• **Empleos de plantilla (funcionarios y personal temporal)**							
• **Personal externo (en unidades de equivalente a jornada completa: EJC)** [57]							
XX 01 02 01 (AC, ENCS, INT de la dotación global)							
XX 01 02 02 (AC, AL, ENCS, INT y JPD en las Delegaciones)							
XX 01 04 ***yy***[58]	- en la sede[59]						
	- en las Delegaciones						
XX 01 05 02 (AC, ENCS, INT; investigación indirecta)							
10 01 05 02 (AC, INT, ENCS; investigación directa)							
Otras líneas presupuestarias (especifíquense)							
TOTAL							

XX es el ámbito político o título presupuestario en cuestión.

Las necesidades en materia de recursos humanos las cubrirá el personal de la DG ya destinado a la gestión de la acción y/o reasignado dentro de la DG, que se complementará, en caso necesario, con cualquier dotación adicional que pudiera asignarse a la DG gestora en el marco del procedimiento de asignación anual y a la luz de los imperativos presupuestarios existentes.

Descripción de las tareas que deben llevarse a cabo:

Funcionarios y agentes temporales	
Personal externo	

[57] AC = agente contractual; AL = agente local; ENCS = experto nacional en comisión de servicios; INT = personal de empresas de trabajo temporal («intérimaires»); JPD = joven profesional en Delegaciones

[58] Por debajo del límite de personal externo con cargo a créditos de operaciones (antiguas líneas «BA»).

[59] Principalmente para los Fondos Estructurales, el Fondo Europeo Agrícola de Desarrollo Rural (FEADER) y el Fondo Europeo de Pesca (FEP)).

En el anexo V, sección 3, debe incluirse una descripción del cálculo del coste de las unidades EJC.

150.3.3. Compatibilidad con el marco financiero plurianual vigente

☑ La propuesta/iniciativa es compatible con el marco financiero plurianual vigente.

☐ La propuesta/iniciativa implicará la reprogramación de la rúbrica correspondiente del marco financiero plurianual.

☐ La propuesta/iniciativa requiere la aplicación del Instrumento de Flexibilidad o la revisión del marco financiero plurianual[60].

Explíquese qué es lo que se requiere, precisando las rúbricas y líneas presupuestarias afectadas y los importes correspondientes. […]

150.3.4. Contribución de terceros

☐ La propuesta/iniciativa no prevé la cofinanciación por terceros.

☑ La propuesta/iniciativa prevé la cofinanciación que se estima a continuación:

En millones EUR (al tercer decimal)

ABE

	2022	2023	2024	2025	2026	2027	Total
Los costes se sufragarán en un 100 % a través de las tasas cobradas a las entidades supervisadas[61]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTAL de los créditos cofinanciados	1,373	1,948	1,748	1,748	1.748	1.748	10,313

AESPJ

	2022	2023	2024	2025	2026	2027	Total
Los costes se sufragarán en un 100 % por las tasas cobradas a las entidades supervisadas[62]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
TOTAL de los créditos cofinanciados	1,305	1,811	1,611	1,611	1,611	1,611	9,560

60 Véanse los artículos 11 y 17 del Reglamento (UE, Euratom) n.° 1311/2013 del Consejo, por el que se establece el marco financiero plurianual para el período 2014-20200.

61 100% del coste total estimado más la totalidad de las cotizaciones al régimen de pensiones del emplead

62 100% del coste total estimado más la totalidad de las cotizaciones al régimen de pensiones del emplea s

AEVM

	2022	2023	2024	2025	2026	2027	Total
Los costes se sufragarán en un 100 % por las tasas cobradas a las entidades supervisadas[63]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTAL de los créditos cofinanciados	1,373	1,948	1,748	1,748	1,748	1,748	10,313

150.4. Incidencia estimada en los ingresos

☑ La propuesta/iniciativa no tiene incidencia financiera en los ingresos.

☐ La propuesta/iniciativa tiene la incidencia financiera que se indica a continuación:

☐ en los recursos propios

☐ en otros ingresos

☐ indíquese si los ingresos se asignan a líneas de gasto

En millones EUR (al tercer decimal)

Línea presupuestaria de ingresos:	Créditos disponibles para el ejercicio presupuestario en curso	Incidencia de la propuesta/iniciativa[64]						
		Año **N**	Año **N+1**	Año **N+2**	Año **N+3**	Insértense tantos años como sea necesario para reflejar la duración de la incidencia (véase el punto 1.6)		
Artículo ….								

En el caso de los ingresos diversos «asignados», especifíquese la línea o líneas presupuestarias de gasto en la(s) que repercutan.

[…]

Especifíquese el método de cálculo de la incidencia en los ingresos.

[…]

63 100% del coste total estimado más la totalidad de las cotizaciones al régimen de pensiones del empleador

64 Por lo que se refiere a los recursos propios tradicionales (derechos de aduana, cotizaciones sobre el azúcar), los importes indicados deben ser importes netos, es decir, importes brutos tras la deducción del 20 % en concepto de gastos de recaudación.

ANEXO

Supuestos generales

Título I: Gastos de personal

Para calcular los gastos de personal se han aplicado las siguientes hipótesis específicas basadas en las necesidades de dotación de personal definidas que se explican a continuación:

- El coste de la contratación de personal adicional en 2022 se calcula para 6 meses en razón del tiempo que se supone necesario para contratar el personal adicional.
- El coste medio anual de un agente temporal es de 150 000 EUR, lo que incluye 25 000 EUR de gastos de *habillage* (edificios, TI, etc.).
- Los coeficientes correctores aplicables a los sueldos del personal en París (ABE y AEVM) y Frankfurt (AESPJ) son 117,7 y 99,4, respectivamente.
- Las cotizaciones al régimen de pensiones del empleador para los agentes temporales se han basado en los sueldos base estándar incluidos en los costes medios anuales estándar, es decir, 95 660 EUR.
- Los agentes temporales adicionales son AD5 y AST.

Título II: Infraestructura y gastos de funcionamiento

La estimación de costes se obtiene multiplicando el número de puestos por la proporción del año en que los puestos estarían ocupados y por el coste de *habillage* (infraestructura) estándar, esto es, 25 000 EUR.

Título III: Gastos operativos

Los costes se calculan con arreglo a los siguientes supuestos:

- Los costes de traducción se fijan en 350 000 EUR anuales para cada AES.
- Se supone que los costes informáticos puntuales de 500 000 EUR por cada AES se repartirían entre los dos años 2022 y 2023 a partes iguales. Se calcula que los costes anuales de mantenimiento a partir de 2024 serán de 50 000 EUR por cada AES.
- Se estima que los costes anuales de supervisión *in situ* serán de 200 000 EUR por cada AES.

Las estimaciones aquí presentadas dan como resultado los siguientes costes anuales:

Rúbrica del marco financiero plurianual	Número	

Precios constantes

ABE			2022	2023	2024	2025	2026	2027	**TOTAL**
Título 1:	Compromisos	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Pagos	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Título 2:	Compromisos	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Pagos	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Título 3:	Compromisos	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Pagos	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
TOTAL de los créditos para la ABE	Compromisos	=1+1a +3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Pagos	=2+2a +3b	1,373	1.948	1,748	1,748	1,748	1,748	10,313

AESPJ:			2022	2023	2024	2025	2026	2027	**TOTAL**
Título 1:	Compromisos	(1)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
	Pagos	(2)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
Título 2:	Compromisos	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Pagos	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Título 3:	Compromisos	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Pagos	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
TOTAL de los créditos para la AESPJ	Compromisos	=1+1a +3a	1,305	1,811	1,611	1,611	1,611	1,611	9,560
	Pagos	=2+2a	1,305	1,811	1,611	1,611	1,611	1,611	9,560

		+3b							

AEVM			2022	2023	2024	2025	2026	2027	**TOTAL**
Título 1:	Compromisos	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Pagos	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Título 2:	Compromisos	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Pagos	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Título 3:	Compromisos	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Pagos	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
TOTAL de los créditos para la AEVM	Compromisos	=1+1a +3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Pagos	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

La propuesta exige la utilización de créditos de operaciones, tal como se explica a continuación:

Créditos de compromiso en millones EUR (al tercer decimal) a precios constantes

ABE

Indíquense los objetivos y los resultados ⇩			2022		2023		2024		2025		2026		2027			
	RESULTADOS															
	Tipo[65]	Coste medio	Número	Coste	Número	Coste	Número	Coste	Número	Coste	Número	Coste	Número	Coste	Número total	Coste total
OBJETIVO ESPECÍFICO n.º 1[66] Supervisión directa de los proveedores terceros esenciales de TIC																
- Resultado				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Subtotal del objetivo específico n.º 1																
OBJETIVO ESPECÍFICO N.° 2																
- Resultado																
Subtotal del objetivo específico n.º 2																
COSTE TOTAL				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

AESPJ

Indíquense los objetivos y los resultados ⇩			2022		2023		2024		2025		2026		2027			
	RESULTADOS															
	Tipo[67]	Coste medio	Número	Coste	Número	Coste	Número	Coste	Número	Coste	Número	Coste	Número	Coste	Número total	Coste total
OBJETIVO ESPECÍFICO n.º 1[68] Supervisión directa de los proveedores terceros																

[65] Los resultados son los productos y los servicios que se van a suministrar (por ejemplo: número de intercambios de estudiantes financiados, número de kilómetros de carretera construidos, etc.).

[66] Según lo descrito en el punto 1.4.2. «Objetivo(s) específico(s)…'

[67] Los resultados son los productos y los servicios que se van a suministrar (por ejemplo: número de intercambios de estudiantes financiados, número de kilómetros de carretera construidos, etc.)..

[68] Según lo descrito en el punto 1.4.2. «Objetivo(s) específico(s)…».'

esenciales de TIC																
- Resultado				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Subtotal del objetivo específico n.º 1																
OBJETIVO ESPECÍFICO N.° 2																
- Resultado																
Subtotal del objetivo específico n.º 2																
COSTE TOTAL				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

AEVM

Indíquense los objetivos y los resultados ⇩			2022		2023		2024		2025		2026		2027			
	RESULTADOS															
	Tipo[69]	Coste medio	Número	Coste	Número	Coste	Número	Coste	Número	Coste	Número	Coste	Número	Coste	Número total	Coste total
OBJETIVO ESPECÍFICO n.º 1[70] Supervisión directa de los proveedores terceros esenciales de TIC																
- Resultado				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Subtotal del objetivo específico n.º 1																
OBJETIVO ESPECÍFICO N.° 2																
- Resultado																
Subtotal del objetivo específico n.º 2																
COSTE TOTAL				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

[69] Los resultados son los productos y los servicios que se van a suministrar (por ejemplo: número de intercambios de estudiantes financiados, número de kilómetros de carretera construidos, etc.).

[70] Según lo descrito en el punto 1.4.2. «Objetivo(s) específico(s)…».

Las actividades de supervisión se financiarán íntegramente mediante las tasas cobradas a las entidades supervisadas, como sigue:

ABE

	2022	2023	2024	2025	2026	2027	Total
Los costes estarán cubiertos en un 100 % por las tasas cobradas a las entidades supervisadas[71]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTAL de los créditos cofinanciados	1,373	1,948	1,748	1,748	1,748	1,748	10,313

AESPJ

	2022	2023	2024	2025	2026	2027	Total
Los costes estarán cubiertos en un 100 % por las tasas cobradas a las entidades supervisadas[72]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
TOTAL de los créditos cofinanciados	1,305	1,811	1,611	1,611	1,611	1,611	9,560

AEVM

	2022	2023	2024	2025	2026	2027	Total
Los costes estarán cubiertos en un 100 % por las tasas cobradas a las entidades supervisadas[73]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTAL de los créditos cofinanciados	1.373	1,948	1,748	1,748	1,748	1,748	10,313

[71] 100% del coste total estimado más la totalidad de las cotizaciones al régimen de pensiones del empleador
[72] 100% del coste total estimado más la totalidad de las cotizaciones al régimen de pensiones del empleador
[73] 100% del coste total estimado más la totalidad de las cotizaciones al régimen de pensiones del empleador

INFORMACIÓN ESPECÍFICA

Facultades de supervisión directa

A modo de introducción, cabe recordar que las entidades sujetas a la supervisión directa de la AEVM deben pagar tasas a esta (costes puntuales de registro y costes recurrentes por la supervisión permanente). Este es el caso de las agencias de calificación crediticia [véase el Reglamento Delegado (UE) n.º 272/2012 de la Comisión] y los registros de operaciones [Reglamento Delegado (UE) n.º 1003/2013 de la Comisión].

En virtud de la presente propuesta legislativa, se encomendarán a las AES nuevas tareas con el fin de promover la convergencia de los enfoques de supervisión del riesgo de terceros relacionado con las TIC en el sector financiero sometiendo a los proveedores terceros esenciales de servicios de TIC a un marco de supervisión de la Unión.

El marco de supervisión previsto en la presente propuesta se basa en la arquitectura institucional existente en el ámbito de los servicios financieros, por la cual el Comité Mixto de las AES garantiza la coordinación intersectorial en todos los asuntos relativos al riesgo de TIC, de conformidad con sus funciones en materia de ciberseguridad, con el apoyo del Subcomité pertinente (Foro de Supervisión) que lleva a cabo los trabajos preparatorios para las decisiones individuales y las recomendaciones colectivas dirigidas a los proveedores terceros esenciales de servicios de TIC.

A través de este marco, las AES designadas como supervisores principales para cada proveedor tercero esencial de servicios de TIC reciben facultades para garantizar que los proveedores de servicios tecnológicos que desempeñan un papel esencial para el funcionamiento del sector financiero sean objeto de un seguimiento adecuado a escala paneuropea. Las obligaciones de supervisión se exponen en la propuesta y se aclaran más detalladamente en la exposición de motivos. Incluyen los derechos a solicitar toda la información y la documentación pertinentes para realizar investigaciones generales e inspecciones, para formular recomendaciones y posteriormente presentar informes sobre las medidas tomadas o las correcciones aplicadas en cumplimiento de esas recomendaciones.

A fin de llevar a cabo las nuevas tareas descritas en la presente propuesta, las AES contratarán personal adicional especializado en riesgo de TIC y centrado en evaluar las dependencias respecto de terceros.

Se calcula que los recursos humanos necesarios serán de 6 EJC por cada autoridad (5 AD y 1 AST para apoyar a los AD). Las AES incurrirán también en costes informáticos adicionales, estimados en 500 000 EUR (costes puntuales), a los que se sumarán 50 000 EUR al año para cada una de las tres AES en concepto de costes de mantenimiento. Un elemento importante en el desempeño de las nuevas tareas son las misiones para llevar a cabo inspecciones y auditorías *in situ*, cuyo coste puede estimarse en 200 000 EUR anuales para cada AES. Los costes de traducción de los distintos documentos que las AES recibirían de los proveedores terceros esenciales de servicios de TIC también se incluyen en la fila sobre costes operativos y ascienden a 350 000 EUR anuales.

Todos los costes administrativos mencionados se financiarán en su totalidad con las tasas anuales cobradas por las AES a los proveedores terceros esenciales de servicios de TIC supervisados (sin incidencia en el presupuesto de la UE).